The Social Construction of Online Fraud

Semire Yekta

Submitted in accordance with

the requirements for the degree of PhD

Goldsmiths, University of London

Department of Sociology

Submission Date: September 2019

Declaration of Authorship

I, Semire Yekta, hereby declare that this PhD thesis, entitled “The Social Construction of Online Fraud,” was carried out entirely by me. Where I have consulted the work of others, this is always clearly stated and appropriate credit given.

Signed: Semire Yekta Date: 20.09.2019

Acknowledgements

This has been an invaluable learning experience and an enlightening journey, through which I have developed personally and academically. I am deeply thankful to many people who supported, encouraged, motivated and challenged me over the past years and without whom it would have not been possible to complete this PhD.

First and foremost, I would like to thank my supervisor Professor Daniel Neyland, who guided me throughout my PhD, provided me with much support and advice and reviewed and commented on numerous drafts over the last three years. I am also deeply grateful to my second supervisor Professor Evelyn Ruppert, for her guidance, support and positivity that helped me to see the good in challenging times.

I am also endlessly grateful to my former employer Martin Königshoven, who not only enabled me to gain access to a very sensitive area of research and research participants, but also never turned down any of my requests despite his busy schedule. He motivated and encouraged me on several occasions to follow the path I had chosen, even if that meant losing one of his well-credited employees. I am profoundly thankful for this support. I also want to thank Mirko von den Benken, who helped me in the recruitment process.

Both Professor Jennifer Gabrys and Dr Jennifer Fleetwood provided me with invaluable feedback on my thesis, and so I am also indebted for their critical but encouraging insights, from which this thesis benefited significantly.

I also would like to thank to my family, my parents, my siblings, and my husband for their endless support and encouragement over the years. They never lost faith in me or in my research despite all the ups and downs of the PhD journey.

Last but not least, I am very grateful to all research participants who were kind enough to spare their time for my interviews after a hard-working day or in their well-deserved lunch breaks, to provide me with invaluable insights and experiences. Without their support, this research would not have been possible.

Abstract

This study critically examines how online retailers aim to differentiate between fraudulent and non-fraudulent customers by using digitally accessible data. Utilising social constructionism and actor-network theory as a theoretical framework, the study argues that online fraud is constructed through social practices as well as technological and organisational relations. This ongoing process involves several human and non-human actors embedded in heterogeneous networks, but the process is not neutral, and neither can the data used as the basis of fraud management be considered value-free. Big data has often been challenged as a neutral representation of reality, given that the collection and analysis thereof involve human biases, choices, selections and preferences. Consequently, the categories of risk assessment and manual fraud management practices represent these values.

However, from a manual fraud review perspective, automated fraud management systems gain an object-like status and often remain unchallenged, and the choices and selections behind these implementations go unnoticed. Categorisations and fraud scorings are pre-giving when manual reviewers enter the risk assessment process and can only operate within existing norms and structures. Manual reviewers take a similar approach and make decisions using additional data sources such as Google and personal and professional websites while imposing their own preferences, biases and understandings, or accepting, rejecting or negotiating alternative realities proposed by other reviewers. It is also crucial how manual reviewers are able to enrol and mobilise other actors to take action in line with their own interests.

The study shows that fraud assessment approaches create their own sense of normality and label those as suspicious or fraudulent who seem to deviate from the norm, thereby leading to the inclusion and exclusion of people. Furthermore, most fraud cases are not reported, which means that the vast majority remain unknown to the police, who then construct their own version of the crime.

This study makes a unique empirical contribution by unravelling the fraud management practices of several online retailers. While companies aim to protect themselves from deception, they are engaged in a number of data-driven, sensitive and partly questionable practices. At the theoretical level, the study suggests that the "social" in social constructionism can no longer be attributed to face-to-face human interactions only but must embrace a new form of connectivity as well as accept that it is enabled and mediated by a number of non-human actors.

List of Figures

1. Introduction

1.1 First Encounters with Online Fraud

About five years ago, I started working for a large customer service provider in Germany and the experience opened up a whole new perspective to me that now represents the basis of this research. The company involved in this study employs about 1,000 people and is a third-party service provider for many online retailers, from very big and international brands, to smaller companies. The service provider handles customer enquiries in relation to online orders, deliveries, refunds and similar issues. As the volumes of customer enquiries are usually high, and retailers often do not have the infrastructure or expertise to manage the variety of calls and emails, the recruitment of service providers has become a better option for them.

My job with this service provider entailed customer care for an international and well-known fashion brand, whereby I would assist customers with their enquiries on a daily basis. Although at the beginning there was nothing particularly surprising about the tasks related to customer services, one duty, namely the manual fraud review, managed by some senior agents, drew my attention. Interestingly, every morning before the lines were open, some employees checked on a number of automatically blocked orders and decided whether these had been placed by fraudulent individuals. It was very interesting to observe how “normal” it was to deal with fraud on a daily basis, alongside other customer services-related tasks, while fraud is a criminal act. After a couple of weeks, I was also "trained" to do the fraud check, which then became part of my daily work. By examining customer details, I had to decide whether I *thought* the customers had possibly used a stolen credit card, a dubious PayPal address or a different payment account for the purchase. Based on customers’ data, personal preferences and experiences, the orders were divided into two categories – genuine customers and fraudulent customers. The line between the two was often very thin, though, given that there are not always distinguishing characteristics about an order so that it fits easily into either of these two categories. It is a simplistic division of customers to manage online orders.

Perhaps many employees would agree that with experience the decisions become easier to make; nevertheless, they are often made on subjective judgements about the customer rather than knowing in advance that the transaction is fraudulent. Consequently, some customers can be assigned a higher risk of committing fraud than others. For instance, is a customer with the name “John Smith” as likely to be labelled a fraudster as somebody with a foreign name? As we shall see later, this is not exactly the case.

Furthermore, the observation also showed that fraud was not only a topic in the morning, but also an issue spread across the day. As customers regularly contact the customer service centre about an order, it is also clear that fraudsters must do so when orders are not delivered as expected. For instance, when agents received a call or an email about an automatically blocked order in the system, they had to make a decision whether to trust the customer and to process the order. How can one decide whether somebody is a fraudster based on a phone call or an email? Does it matter what the customer sounds like? Whether they sound confident? Whether they are clear about what they ordered? Whether they sound English? Because the voice or the text can sometimes be the main basis on which to make a decision for or against a person.

After some months of observation and active fraud "detection," I decided that this could be a very interesting and valuable area of research. When I stressed my research interests to my former employer and its possibility was being examined, I was very fortunate that one of our clients, with a volume of more than 19€ billion sales annually, decided to set up a new team for the online fraud management of this very large and well-known international fashion brand. Given my research interests, I was one of the first people on board and was managing fraud with a more advanced system servicing many European and North American countries. Interestingly, there were many similarities between the fraud management approach of the first and the second online retailer and, as the research later shows, of many other online stores. Overall, four years of observation and active participation in different stages of fraud management as an agent, a team leader, a supervisor and a fraud expert made clear

that fraud management is not a straightforward process whereby fraudulent individuals can be identified easily, before or at the time of committing fraud.

It is also noteworthy that it took about 11 months, given the sensitivity of the data, to receive permission from my former employer to conduct the research. Furthermore, the experience with online fraud and self-reflection as a participant and an observer meant including the additional research method of auto-ethnography. The research process, methods, access to the participants and ethical clearance granted by the university will be highlighted in more detail in the methodology chapter. The next section will explore how online fraud can be defined and understood in relation to specific realm of cyberspace.

1.2 Defining Online Fraud

Fraud has been part of society for centuries and is probably as old as human history itself (Montague, 2010; Button and Cross, 2017a). While fraud exists in different forms and variations, fraudulent activity can be considered an act of deception, as its perpetrators need to conceal their own identities or intention to commit a criminal offence. One definition of fraud is provided by Stamler et al. (2014, p. 15-16), who state that:

> **Fraud includes the commission of any act of deceit, deception, or the submission of false information or material that is designed to obtain some advantage or benefit. In other words, fraud is any form of artifice, contrivance, guile, treachery, concealment, or disguise intended to induce another to part with money, property, or other legal rights, unjustly or unfairly.**

While this definition can be applied to various forms of fraudulent action, online fraud also needs be understood in relation to cyberspace. An extended definition in this regard is offered by Levi et al. (2017), who contend that online fraud is fraud with a cyber dimension, as it takes place within the specific realm of cyberspace. It is important to understand how the digital environment enables and shapes criminal

activities, since online fraud has become a significant form of deception because of new technologically mediated and anonymous processes.

The understanding of cyberspace that is relevant to and adopted in this study addresses how it is made up of relations between people and technologies of the internet. First, one of the most important characteristics of cyberspace is the construction of a unique form of connectivity. As Mlambo (2013, p. 9) points out, the '*Internet is a network of networks, and these networks are interconnected to each other in different configurations*'. Further, it creates a type of connectivity, a platform for interaction (Holt et al., 2017) that enables people to get involved in activities without being in direct contact (Wall, 2007). Individuals are assembled in cyberspace, engage which each other and participate in various forms of action while being physically in completely different locations. This is a fairly important point in understating online fraud, because as opposed to "offline" crimes, the victim, the target and the offender no longer share the same physical space but are part of the same event, which in turn creates a unique environment and engenders challenges that cannot be solved through traditional crime prevention and detection methods.

Second, the internet provides and creates a sense of anonymity (Moore, 2014; Wall, 2007) whereby people can conduct criminal activities at a distance while hiding their real identities (Brenner, 2012). This can also be linked to the previous point, since when the same physical space is not shared, it becomes more difficult to be aware of all actors involved and of the identity of these actors. While placing an order online or making an online transaction, therefore, it is not necessarily possible to be aware of all processes running in the background or of other human and non-human participants – or intruders – involved in the process.

Third, in addition to remaining anonymous, cyberspace allows people to conceal their real identities, to embody alternative identities and impersonate others with a view to committing crime (Clough, 2010). Within the cyber environment, it is challenging to know whether people are who they claim they are, and arguably this is one of the main issues for online retailers, because a great deal of fraud is conducted by

concealing one's real identity and taking the identity of others. For example, when an online order is placed using somebody else's username and password, address and payment details, the order can look to online retailers like any other normal transaction. Given that there are no requirements to show an ID, credit or debit card to proceed, anybody can enter false information and generate alternative identities, which they can then use to commit fraud.

The relations between people and technologies create consequences. For example, when online fraud is perpetrated, there is usually no immediate evidence, as opposed to traditional crimes such as burglary, where the damage is immediately and clearly visible (Button and Cross, 2017a). For instance, a cardholder might simply not be aware that their payment details have been stolen and used for an online order unless they check their bank statements regularly. Even then, it takes some time before the unauthorised payment appears on bank or credit card accounts, which can then be too late to take action and prevent the damage. The delayed notification of online fraud not only makes it more challenging to stop the fraudulent transaction on time but also to successfully track down the criminal.

Additionally, the internet maximises the extent and scope of online fraud. The connectivity between millions of people, companies and organisations makes it possible to commit crime on a grand scale. Going back to burglary as an example, an individual or group of individuals would face limitations when targeting a bank or a shop, because they can only attack one or a small number of victims at once and can only gain access to a limited amount of funds that are physically available. However, online criminals are able to target millions of people at the same time and cause damage to a greater extent. Furthermore, online fraudsters can use the same stolen identities and payment details to place orders on different e-commerce platforms, which in turn leads to multiple victimisation.

1.3 Online Fraud in E-commerce

Traditionally, retailing entails the exchange of goods and funds in a store environment, where customers and shop employees or owners share the same

physical space and can communicate face-to-face. Before making a purchase, customers can view products and check their quality, while the shop owners and employees are able to see the customer and the physical possession of the payment card before processing with the transaction. Although this might sound old-fashioned and somewhat commonplace, this is a very important point to note when differentiating between offline and online retailing – online orders are usually placed over the internet, where it is not possible to see either the customer or the payment card. As pointed out earlier, the internet connects people and companies across locations and borders, and so with retailing moving online, retailers are no longer dealing with locals but with people from across the globe. The lack of a shared physical space between the customer and retailers makes it difficult to know who is at the other end of this exchange process and whether the people are really who they claim to be.

Online fraud often entails using the identities and payment details of others to make an online purchase. However, when such an exchange takes place, there is usually no immediate proof that a crime has been conducted; for example, if a fraudster abuses a person's name and payment details, the shop will not necessarily be aware of the misdemeanour at that very moment, unless it comes to their attention, such as when the victimised individual reports it. However, as it usually takes some time until an unauthorised payment appears on a bank statement, it can often be too late until the victimised individual notices the payment and informs the bank or the online retailer, there is not much the retailer can do afterwards. In such cases, retailers lose their products and must return the funds to the actual cardholder. Consequently, online retailers have a profound interest in preventing online fraud, because they are usually liable for the matter, as they accept so-called "card not present" payments (Montague, 2010).

While active and efficient fraud prevention is crucial for online retailers seeking to reduce financial loss, fraud simultaneously, and for several reasons, represents a major challenge. First, retailers cannot easily identify the difference between genuine customers and those who are disguised as such. If we turn to the definition of fraud above and reiterate that it is a form of deception, how can we then possibly know in

advance which of the transactions are fraudulent and which of the customers are veiled impostors? Second, online fraud prevention requires a good understanding of the phenomenon and of advanced tools, technologies and techniques. To respond adequately to the complexities and entanglements of fraud in cyberspace, retailers need to become experts, private police officers and detectives; however, this can be an overwhelming process, because this involves asking them to move beyond providing a service to customers and instead accepting and dealing with technologically mediated forms of criminal activity as a part of their business.

Third, when online retailers take preventative action against online fraud, they might find themselves entangled in a dilemma as to whether sales or a reduction in such offences should be the priority, because fraud prevention will inevitably result in a bad customer experience, dissatisfaction (Bamfield, 2012) and eventual loss of revenue. This is not only because additional measurements need to be implemented and will cause delays in order processing, but also because these measurements are calculations of risk and simple estimates while using limited available digital data sources (Johnson, 2013). While it is clear that online retailers implement pre-emptive measurements to reduce fraud rates, these can also lead to false positives, i.e. transactions that are not fraudulent but are labelled as such, as they have some of the same characteristics (Vona, 2017). This means that there is not a simple method or technology in place that can easily identify fraud in cyberspace. Although companies either spend large amounts of money on developing the most advanced detection technologies or use this money to reduce fraud rates, there is no perfect solution that will help them clearly identify criminal individuals.

1.4 Understanding Chargeback

The previous sections highlighted that online retailers need to have a profound understanding of advanced technological tools as well as knowledge on the specificities of cyberspace, to run a fraud prevention system successfully. Moreover, fraud prevention and detection entails reviewing online transactions automatically and manually on a daily basis and then deciding which customer is genuine and which

is not so. As this is a proactive assessment, retailers can often not be sure at that stage whether their assessments are correct, and a crime can only be "proven" when a retailer receives a chargeback in relation to a particular order. This means that while retailers cannot be fully sure that all accepted transactions were actually genuine, some of these accepted transactions will later become fraud cases as a result of chargeback.

Chargeback can be understood as the return of funds to customers by their issuing bank, based on the claim that they did not make or approve a transaction (Montague, 2010). It is important to understand chargeback for two main reasons. First, it means for the retailers that they have accepted a number of fraudulent transactions as genuine. While the transaction might have looked "normal" and might not have any characteristics that could be defined as suspicious so that it was approved, the notification of the cardholder is accepted as proof that the assessment was incorrect, and a fraudulent transaction was approved. Second, chargebacks mean costs for retailers. When a chargeback is issued by the cardholder through the issuing bank, the retailer is asked to pay. Merchants can even receive a chargeback six months after the purchase was made, which usually they must reimburse (Ward, 2010).

In addition to fraud claims, there are also chargeback disputes, due to dissatisfaction with goods or services, such as for not receiving a purchased item, receiving an item not meeting quality expectations, technical issues or due to a misunderstanding with the retailer. In such cases, the funds can also be returned to customers' accounts by their issuing banks (Montague, 2010; Lee and Scott, 2017; Samet, 2013). However, from the fraud management perspective, it can be challenging to know whether the chargeback was received due to fraud or customer dissatisfaction, although the vast majority of chargebacks are related to the former. For example, if the customer opened a chargeback dispute due to other reasons, it is possible that they will be categorised as fraud.

Chargeback regulations give a higher priority to customers rather than retailers, which means that merchants must take the responsibility for fraud and reimburse the cardholder. As online retailers accept card not present payments through debit or credit cards, the costs of fraud are shifted to them (Savage, 2012; Chaudhary and

Mallick, 2012). Challenging or reversing chargeback is often not possible for retailers, so they need to cover fully the costs of fraud, which can include returning the payment to the cardholder, the cost of the goods, shipping costs, card association fees and penalties, chargeback and administrative fees (Chaudhary and Mallick, 2012). For this reason, it is in the interests of retailers to avoid chargeback as much as possible.

As the following chapters will show, many elements are involved in fraud management practices in an attempt to predict and prevent this form of online crime. However, whether or not fraud has been successfully committed is based on received chargeback claims. Therefore, chargebacks are essential to fraud management, because they are considered the main indication of fraud. As will be detailed in Chapters 4 and 5, chargebacks are decisive in categorising customers as genuine or fraudulent, and in the decision-making process.

1.5 Understanding the Significance of Data

Online fraud results from the misuse of personal and transactional data. Similarly, fraud prevention is also grounded profoundly in the assessment of data – also referred to as big data – which can be understood as the collection and management of large amounts of digital data generated through the engagement with organisations, businesses, governments and other agencies (Gregory and Glance, 2014), the aim of which is to recognise trends or patterns and predict future behaviours (Payton and Claypoole, 2014). Fraud prevention and detection would not be possible without using customer data to generate features and labels and then use these to create categories of genuine customers and those who are not so genuine. Therefore, data is an important element when researching online fraud. Chapter Two will explore in depth the significance of data.

1.6 Online Fraud as a Social Construct

This study examines how online retailers aim to differentiate between fraudulent and non-fraudulent customers, by using automated and manual detection methods. Furthermore, it takes a sociological view on online fraud and argues that it is a social construct. This notion is based on the core idea that we cannot know but only assume what constitutes fraud. In addition, the following chapters will demonstrate that it is not based on legal definitions, police records or victimisation surveys used in most criminology studies, but rather emerges from fraud actors' own assessments – how it is assessed and managed leads to a variety of constructions.

The theoretical orientations guiding this research are social constructionism and actor-network theory (ANT). The social constructionist perspective challenges the taken-for-granted understandings of online fraud that accept it as something given, obvious or factually determinable (Berger and Luckmann, 1966). Furthermore, it provides the theoretical framework to demonstrate that this crime is the result of social practices (Henry, 2009); however, social constructionism provides a narrow understanding of the "social" that only focuses on human actors, while human actions are often enabled and mediated by non-humans (Law, 2008; Dolwick, 2009). As fraud involves people, organisations, data, devices, content and digital connectivity between various heterogeneous actors, actor-network theory is also employed to acknowledge and unravel all of the bits and pieces that come together in the making of online fraud, as well as to explore relations between people and technologies of the internet. This research suggests that in order to understand online fraud fully, we must consider the processes and the conditions through which the social reality of online fraud turns into something measurable, something definite.

This study explores particularly manual fraud prevention and detection. A manual review represents the final step in fraud management and involves human actors who actively make selections and choices on transactions and make decisions on whether these should be labelled as genuine or fraudulent. These manual reviewers

not only have the power to make clear distinctions between customers, but they can also override or overrule automated fraud decisions and re-categorise customers. For this reason, the manual review process is an essential part of fraud detection and prevention and therefore the focus of this research. Although some insights into the automated identification of fraud and decision-making will be provided, this research does not aim to examine algorithms per se, but it will show partly how the automated and the manual are interrelated. The main aim is to provide crucial empirical insights into the process of fraud management.

1.7 Study's Contribution to Knowledge

Many studies in the literature point out that there is a need to conduct critical studies on online fraud in relation to the digital age. For instance, Kitchin (2014a) suggests that it is important to research the social, ethical, legal and political implications of the data revolution, given that very few studies have been conducted to explore specifically cyberspace. Moreover, Crawford et al. (2014) highlight that we need to carry out critical research to scrutinise big data's position as a neutral representation of the social world. In relation to online fraud, Williams and Levi (2012, p. 269) note that:

> **These findings call for a more in-depth qualitative understanding of the cooperation between eCrime controllers and their data consumption practices. Ascertaining what shapes this cooperation (and non-cooperation) and how perceptions compare with 'actual' threats and risks is necessary if we are to better understand the 'social construction' of the problem and subsequent policy and operational outcomes.**

Despite its significance, researchers often lack transparency or access to bridging the gap in the literature. For instance, Nisbet et al. (2009) argue that there is very little information available on fraud detection modelling, since such information is not publicly shared for different reasons. Similarly, Pasquale (2015) underlines that we are unable to gain access to the decision-making processes of companies because such practices are kept secret – we only see the inputs and outputs but are unable to

look into the calculations, risk scorings and decisions. This lack of access and knowledge makes it difficult to understand the basis of algorithms (Chan and Moses, 2016) and fraud prevention systems.

This study makes a distinctive and unique contribution by addressing the gap identified in the academic literature. The critical insider view, in combination with a qualitative research method, enables a rich perspective on the process of the identification, determination and detection of online fraud as well as on its social and ethical implications. This research's main contribution will be to open the black box of the manual identification and categorisation of fraud, subjective and collective social practices and their relation to technological and organisational entities and to provide new empirical insights into the process of how online fraud is constructed.

1.8 Thesis Outline

The thesis is divided into eight chapters. The content of subsequent chapters is structured as follows.

Chapter Two is the literature review and consists of four main sections. The first section provides an overview of relevant literature on both cybercrime and online fraud, as the latter can be considered a sub-area of the former. It shows that while there is a growing body of literature on some areas of cybercrime, there is only limited research available on online fraud (Yar, 2013, Owen et al., 2017). The first section of this chapter identifies gaps in the literature which this research addresses with the selected theoretical framework.

In the second section, two theoretical orientations, namely social constructionism and actor network theory, are explored, as they represent the theoretical foundation of this research. Starting with social construction, the historical development of constructionist perspectives is examined, and it is outlined how social construction has become a powerful theoretical orientation in understanding social realities (Burr, 2015; Restivo and Croissant, 2018; Gergen, 2015). The section then addresses prominent themes and current debates and discusses them in relation to online fraud. One of the main arguments emerging from the literature is how everyday

knowledge is produced and maintained through language (Berger and Luckmann, 1966; Gergen, 2009). This important point is particularly explored in the empirical Chapter Five, indicating that language plays a crucial part in creating a common-sense understanding on online fraud in team and collective decision-making processes (Burr, 2015; Gergen, 2015). This is then followed by the social construction of scientific knowledge. Traditionally, science is considered a process of discovery. Social constructionism, however, takes a critical stance on scientific knowledge and argues that all knowledge is a process of production, which also applies to how knowledge on online fraud is constructed. Some of the critical perspectives on the social constructionism of scientific knowledge such as the study of Latour and Woolgar (1979) conducted in a laboratory have given rise to the development of actor-network theory (ANT) (Law 1992, 2008; Dankert, 2011). Latour and Woolgar drew attention in their research to the process of knowledge production within the laboratory and how statements were negotiated before they turned into 'facts'.

The Actor network theory suggests that the world needs to be understood as a relational effect whereby human and non-human entities come together in the making of social realities (Belliger and Krieger, 2016; Law, 2008; Tatnall, 2001; Roberts, 2012). ANT makes an important theoretical contribution by extending the social to non-humans, which are particularly relevant for this research, as online fraud is enabled by and mediated through technological developments.

The third section in this chapter explores how crime can be understood as a social construct. While crime as a social construct is not a new idea, the section demonstrates that labelling perspectives particularly have become prominent within the literature (Polizzi, 2015; Henry, 2009; Rosenfeld, 2010; Czabanski, 2008; Becker, 2008; Eglin and Hester, 2013; Christie, 2004). These labelling perspectives, however, focus mainly on face-to-face interactions and do not consider the role of non-humans, such as technologies or data, or digital forms of communication and connectivity (Becker, 2008). For this reason, the section suggests that while constructionist perspectives provide a critical perspective on crime, they are not able to deal with new forms of criminal activity such as online fraud that have emerged as a result of technological developments. As the section shows, the inclusion of ANT as

a theoretical orientation, particularly consideration of data as actor-networks, is beneficial in developing a better understanding of how online crimes are constructed. In the final section, the review of the literature leads to the identification of a key research question on how online fraud is constructed through social practices and technological and organisational relations, accompanied by four additional sub-questions.

Chapter Three demonstrates the methodological framework of this research. It starts by providing an overview of selected research methods and designs and discusses them in relation to this research's questions and objectives. This work benefits from a mixed method approach, as it combines semi-structured interviews with auto-ethnography. While 32 in-depth interviews were conducted with call centre and fraud agents, supervisors, managers and the police, to gain crucial insights from the people who deal with the issue on a daily basis, working professionally in the area required the inclusion of auto-ethnography as an additional research method. The chapter highlights that, arguably, being an insider was the most crucial factor in this study, because it not only created interest in choosing this area of research, but also gave rise to how the study was designed and conducted, access gained, and participants recruited. Additionally, it is outlined how being an insider enabled the provision of more depth and breadth in this research while inevitably also creating challenges and ethical dilemmas (Bailey, 2007; Galletta, 2013; Teusner, 2015). It is shown how these challenges and dilemmas were addressed, as well as issues such as ethical clearance, by the university, my former employer and the participants.

Chapter Four, the first empirical chapter, examines how online fraud is constructed through the identification and categorisation of people based on their personal and transactional data. As outlined previously, online fraud prevention results either from an automated or a manual approach to data. The chapter starts with providing some background information on how both approaches are interrelated. This relationship between the automated and manual methods shows that both need to be considered in combination, as they both affect how the other system operates. While automated rules determine the structures and the framework within which the manual review can function, manual practices can also change automated systems through so-called

"black-and-whitelisting." Blacklisting refers to the process of blocking users so that they cannot place any new orders using the same data while whitelisted customers are ensured that they can place as many orders as they like without being stopped or scrutinised.

The chapter then argues that the manual identification of fraud is facilitated through several features, including categorising customers by the consistency of their data and trends emerging from their past transactions. While the consistency of data is considered a good sign, any inconsistencies can be viewed as suspicious or fraudulent. Customers are also categorised depending on their payment methods, as not all are associated with the same degree of risk; for example, while a credit card payment can be considered as risky, customers choosing PayPal as an option will face less scrutiny and suspicion. Other important features include the housing, area and country of residence, which means that customers can be considered genuine or fraudulent depending on the type of housing and area in which they live. Moreover, area is also linked to the social and ethnic background of customers, which implies that people with foreign names and living in socially diverse areas will have a higher chance of being categorised as fraudulent. The chapter concludes that the assessment of customers based on their background, ethnicity and order detail characteristics creates categories of inclusion and exclusion. While it is mostly not possible to know in advance who is genuinely criminal, some customers will be labelled as such and excluded as a result of previously identified groupings and labels.

Chapter Five will draw upon Berger and Luckmann's original work on the social construction of reality (1966), which argues that all human knowledge is constructed in social practices. The chapter illustrates empirically how manual practices are developed, maintained and negotiated in fraud management teams. The chapter consists of two main sections. The first section of Chapter Five details how fraud agents develop and maintain a set of internal fraud practices to differentiate between genuine and fraudulent customers. It demonstrates once more that customer data is crucial in generating fraud practices (boyd and Crawford, 2012; Andrejevic, 2014). However, while agents use available datasets from past and present transactions to create an understanding on fraud, the data do not always suffice to make clear

distinctions, in which case agents also rely on their personal judgements. It is outlined that, in some cases, agents consult their colleagues when they have doubts about whether to accept a transaction, so decision-making can then become a form of group discussion in which different arguments are weighed up and various understandings are negotiated. Another common practice amongst fraud management team members is order cancellations, which do not necessarily result from a clear suspicion of fraud but when the agents feel that there are not sufficient reasons to accept the order. In such cases, order cancellations can instead act as an experiment to test customers' reactions. If the customer gets in touch and complains about the cancellation, the next order is then usually accepted.

The second section of Chapter Five outlines external practices that become necessary when internal practices are insufficient to make decisions. External practices consist of a Web search and phone validation. With the former, agents aim to find more information about customers on the internet when decision-making remains a challenge after reviewing internal datasets. This practice usually starts with running an online Google check on a customer to access additional data sources, which often leads to other webpages such as social media and phonebooks, where fraud team members can compare internal and external datasets while looking for a match. The goal is to find external validators who can confirm that the customer is who they claim they are. As will be shown, this practice raises major ethical questions, given that customers are judged without their consent or knowledge based on publicly accessible and available information.

In addition, as not all customers can be identified easily through a Web search, fraud management team members use the final step of phone validation to make a decision. This usually entails a fraud team member confronting the customer with some questions on the phone and using the answers and reactions of customers as the basis of their assessment. The chapter concludes that decision-making based on available data can be challenging, so fraud management has to move beyond traditional resources and embrace other publicly accessible datasets to differentiate between genuine and fraudulent customers. While external resources are helpful, they do not always provide the answers needed to make fraud decisions.

Chapter Six shifts the focus to actor-network theory to examine the relationship between human and non-human actors which come together in the making of online fraud. The chapter details how online fraud is partly the effect of associations between human and non-human actors embedded in heterogeneous networks (Law, 2008; Callon, 1998). While the previous two chapters focused on fraud management team members, data and fraud technologies, Chapter Six considers the human actors within wider network relations, as they do not act on their own but in relation to other actors. This chapter is divided into two sections. The first section presents an assemblage of heterogeneous actants within the customer service centre and discusses how the relationships between fraud agents and another set of actants influence and constrain fraud practices. These include contracts, a limited training process, time constraints and multiple roles and pressures. The second section examines network relations between the customer service centre and a number of other entities. While fraud agents look into datasets and attempt to distinguish between honest and dishonest customers, their decision-making takes place within a wider context and in relation to other actors, such as customers, departments, clients and organisations. The chapter shows that what determines something as fraud is also influenced by people who mobilise or fail to mobilise other entities to take action. The chapter concludes that customer services as an actor-network is entangled in other actor-networks, and how these actor-networks come together creates different forms of fraud constructions.

Chapter Seven is the final empirical chapter and focuses on another set of actor-networks – online retailers and police – and examines their associations with customer services and policing online fraud. This chapter is also divided into two sections. The first section of this chapter provides insights into the actor-networks of online retailers, who deserve specific attention because while they recruit service providers to handle customer enquiries, they also relate to fraud management by defining roles, responsibilities and targets, as well as making decisions on the scope of fraud practices. Fraud agents as actors can only operate within a framework that has been defined by the online retailer, as they are the "owners" of the physical and digital goods through which several practices come together. As all decisions are relational, online retailers also make decisions and rationalise them based on cost

assessments, resources and capacities. The second section of this chapter demonstrates how retailers and police are not able to align their objectives and how this influences what becomes fraud. While retailers do not report fraud, due to the cost of making an assessment and the low chances of success, many cases remain unnoticed by the police (Levi et al., 2017; Wall, 2007 /10), thereby leading to a particular construction of online fraud and the possible negligence of policing it.

Chapter Eight is the conclusion and is divided into four main sections. The first section reiterates the research questions and outlines how they were answered throughout the empirical chapters. The research is grounded in one main and four sub-research questions. It is also demonstrated in this first section how each empirical chapter aimed to address one sub-question. The second section of this chapter discusses the contributions of this research. Starting with theoretical contributions, it is illustrated that this study extends the theoretical work of other researchers in social constructionism and actor-network theory. It is also highlighted that social constructionism does not just happen but is a complex process involving many heterogeneous actors (people, preferences, data, individual decision-making, collective evaluation, organisational roles and structures, victims, financial institutions and the police). This also means that the social can no longer be limited to face-to-face interaction or human relations but must be extended to the technologically mediated interaction and connectivity as well as non-human actors to be able to understand how online fraud is constructed.

The second contribution of this research is methodological. While the limited research on online fraud and cybercrime in general is grounded on a lack of access to, and understanding of, the technicality of online crimes, the section demonstrates that, in my case, being an insider was fairly crucial in overcoming these obstacles; in fact, the research benefited significantly from existing good relationships and the trust within the workplace to the extent that the service provider granted access to a very sensitive area of research. Furthermore, a working knowledge on online fraud management provided a profound understanding of the technical side of online fraud so that this obstacle could also be fully addressed. The third and main contribution is empirical, as the research provides in-depth and unique insights into the online fraud

prevention and detection methods employed by a service provider and several online retailers, and it outlines how online fraud results from social practices, people and things.

The third section of Chapter Eight details the limitations of the research, as each study naturally has some drawbacks. It is outlined that the interviews were conducted before defining the theoretical basis of this study, as it is often the case with qualitative research. As a result, some questions appeared after detailed engagement with theory, so it could have been beneficial to pose these questions in the actual interviews. A further limitation emerges from the fact that most of the data were collected within the same organisational setting with similarities in fraud management practices, even though employees working for different online retailers were interviewed. Furthermore, another limitation of this study is that it only provides limited information on automated fraud prevention practices. While the aim was not to specifically explore automated systems, the research would have certainly benefited from wider insights into automated classifications. The fourth section and final section of Chapter Eight then addresses the implications of this study for future research and practice.

2. Literature Review

2.1 Introduction

This chapter consists of four main sections, the first of which critically examines relevant literature on cybercrime and online fraud. The choice to focus more generally on cybercrime resulted on the one hand from the limited research, which looks specifically at online fraud, and on the other hand because criminal activities that fall under both terminologies often overlap. The section assesses the current stage of research and identifies limitations, which this study aims to address through the selected theoretical and empirical framework.

The second section discusses the two theoretical orientations of social constructionism (Berger and Luckmann, 1966) and actor-network theory (Latour, 1996; Law and Callon, 1988) that build the theoretical foundation of this research. Starting with social constructionism, historical developments are examined, prominent themes and debates are identified and then discussed in relation to online fraud. One of the main themes addressed in the section is how language is used to construct and maintain common-sense understandings and everyday knowledge (Burr, 2015). This is followed up by the social construction of scientific knowledge, which indicates that scientific knowledge – as with everyday knowledge – is also a process of production (Latour and Woolgar, 1979). The section argues that critical studies of science and technology have given rise to the development of actor-network theory (ANT) which provides a more holistic approach to online fraud by including non-human actors.

The third section shifts the attention to crime – albeit to those studies which take a constructionist approach – to examine to what extent social constructions inform crime-related studies in the contemporary literature. Much empirical research in this area uses face to face interactions, drawing on the labelling perspective while exploring crime from a constructionist viewpoint (Becker, 2008; Christie, 2004; Polizzi, 2016), while studying cybercrime and particularly online fraud require researching technologically mediated forms of interaction and connectivity. Thus, the prominent discussions do not necessarily take into account the role of technology in

crime constructions. Consequently, the section explores how contemporary constructionist perspectives can be extended through the inclusion of ANT and data as a crucial non-human assemblage. In the final section, a brief overview of the insights gained from the literature is provided and the key research questions identified.

2.2 Cybercrime

Cybercrime can be considered an umbrella term that refers to a variety of heterogeneous illegal and illicit activities in cyberspace (Wall, 2015; Grabosky and Smith, 2003; Yar, 2013; Wall, 2007 /10). As Wall (2017) points out, while most people would agree that cybercrime exists, there is only sparse consensus on what actually constitutes cybercrimes. This is also because cybercrime studies emerge from various disciplines such as sociology, criminology, business studies and computer sciences (Yar, 2013; Holt, 2016). The diverse range of approaches makes it more challenging, on the one hand, to find a starting point (Yar, 2013) and on the other hand to see the overall picture and make accurate assessments and comparisons between varying studies of the subject (Kshetri, 2010).

The current literature does not provide a consistent definition of cybercrime (Yar, 2013), because not only do academic disciplines vary in their understandings of criminal activities in cyberspace, but also each country and jurisdiction have its own definition; for example, while some acts are considered a form of cybercrime in one jurisdiction, this might not be the case in the other (Kshetri, 2010). Similarly, some definitions of cybercrime refer specifically to acts that are defined as illegal by law, while others take a broader perspective by also including harmful behaviour. For example, Chawki et al. (2015) define it as "*unlawful acts wherein the computer is either a tool or target or both*" (p. 3). However, according to Yar (2013), cybercrime also entails acts that might not be illegal per se but are nevertheless considered deviant by the majority of people in society. Additionally, according to Oxford Dictionary (n. d.) cybercrimes are *"Criminal activities carried out by means of*

computers or the Internet." The varying definitions generate different understandings on what constitute cybercrimes.

Another main point emerging from the literature is the question as to whether cybercrimes have moved into cyberspace, i.e. where old crimes are committed with new tools, or whether they represent new crimes. In fact, much of the research considers criminal activities in cyberspace as a combination of traditional and new crimes which come into being as a result of newly developed technologies (Brenner, 2012; Button and Cross, 2017a; Wall, 2017). For example, Brenner (2012) outlines that crimes might have remained the same, but the tools changed, while at the same time, new forms of criminal activities have emerged which would have not been possible without the proliferation of the Internet (Grabosky and Smith, 2003) and the opportunities it has created (Wall, 2017). Furthermore, Button and Cross (2017a) highlight that crime rates have not decreased, despite the official statistics which indicate otherwise, but have simply moved online.

Despite these variations, cybercrime-related studies could perhaps be united in the sense that they rather take an offence-based approach and do not study offenders or victims (Wall, 2015). This notion becomes particularly apparent when assessing how researchers aim to categorise crimes in cyberspace. A well-cited source is Wall (2007 /10), who differentiates between three groups, namely computer integrity crimes, computer-related crimes and computer content crimes. The computer integrity crimes refer to criminal activities that aim to access illegally a computer or a network. These activities include hacking, denial of service or spying. The computer-related crimes consist of criminal activities that are committed with the aid of a networked computer, such as phishing or various forms of fraud, while computer content crimes assemble the dissemination or trade of various types of offensive content. Another way of categorising cybercrimes is to distinguish between cyber-dependent and cyber-enabled crimes (McGuire and Dowling, 2013; Leukfeldt, 2017). Cyber-dependent crimes refer to new types of offending which exist due to the existence of computers, while cyber-enabled crimes, such as traditional crimes, could also be carried out if computers did not exist, albeit the technology increases the

extent and scope of such offending. In both offence-based categorisations of cybercrimes, there are overlaps between each group.

Furthermore, the cybercrime literature focuses on some selected areas, while others are neglected (Yar, 2013, Owen et al., 2017). For example, much of the research focuses on technical aspects and the development of technological tools and methods to combat cybercrime, mainly emerging from fields such as computer sciences (Holt, 2016; Leukfeldt, 2017), while other studies carried out by social scientists concentrate on human actors and provide limited understanding of the technological aspects thereof (Holt, 2016).

In the cybercrime literature, different terminologies are used to describe fraudulent activities on the Internet. These include “cyber fraud” (Button and Cross, 2017a), “payment fraud” (Johnson, 2013), “online payment fraud” (Wells, 2010), “internet scams and frauds” (Singh and Davidson, 2015), “card-not-present fraud” (Montague, 2010; Wall, 2007) and “order fraud” (Bamfield, 2012). In fact, Action Fraud’s list of online frauds entails 30 different forms of fraudulent activities, including auction and shopping fraud, lotteries, loans and work-from-home scams. These terminologies are often used to describe the same or similar forms of fraudulent action. For example, card-not-present fraud or payment fraud often refer to the same fraudulent activity and are used interchangeably, while cyber frauds and scams can go beyond payment-related fraud. Additionally, a great deal of research on online fraud is carried out by people with a business background and not academics (Montague, 2010), whose main aims are to promote their own economic interests and remain competitive in the market.

Furthermore, there are some official and corporate sources of data which shed light on cybercrime statistics and figures. In England and Wales, in regard to fraud and computer misuse, there are mainly two sources of data used for official statistics. These are The Crime Survey for England and Wales (CSEW) and the National Fraud Intelligence Bureau (NFIB) by Action Fraud which is the national reporting centre for fraud offences and cybercrime with a financial motivation. Action Fraud collects reported offences of computer misuse and fraud in relation to the public and businesses, whereby it makes a distinction between online and offline fraud, and

computer misuse. Prior to Action Fraud, the police recorded these offences. Action Fraud was introduced as a result of deficits in recording practices of the police, their lack of understanding in what constitutes fraud, as well as their willingness to accept reports. Moreover, the official statistics also benefit from industrial sources such as Cifas and Financial Fraud Action UK which report fraud when their member organisations are victimised (Office for National Statistics, 2018; McGuire and Dowling, 2013). The Office for National Statistics (2018) estimates 4.7 million incidents in regard to fraud and computer misuse in England and Wales in the first nine months of 2017. Compaing these figures with 272,980 offences recorded by Action Fraud shows that there is a large difference between recorded offences and estimated numbers of fraud and computer misuse.

In addition to official statistics there are a number of industrial reports which give insights into the cybercrime statistics and numbers affecting individuals. In fact, industry reports provide a considerable amount of information on cybercrime (McGuire and Dowling, 2013). For instance, a comprehensive study conducted by Norton by Symantec Corporation (2018) examined the impact on cybercrime in 20 countries. The report suggests that 978 million people from 20 countries were victimised by cybercrime in 2017; this makes 44% of consumers. It was outlined that countries such as China (352.70 m), USA (143.70 m) and India (186.44 m) have the highest numbers. However, the victimisation rates in Germany (23.36 m) and the UK (17.40 m) are also fairly high.

According to the study of Symantec Corporation the most common forms of cybercrime experienced by individuals were an infected device though a virus or other cyber security attack (53%), payment card fraud (38%), compromised account password (34%), compromised email or social media account (34%), online purchases made through fake or fraudulent sellers (33%), and opening a fraudulent email or responding by providing sensitive data (32%). The report also outlines that consumers lost $172 billion on a global scale and on average $142 while also spending almost three full workdays to deal with the consequences of fraud afterwards.

Another form of fraud not included in this report, but which increasingly affects individuals, is romance fraud, defined as:

A fraud technique that criminals use to access their victims' finances by engaging in a romantic relationship with them, gaining their trust and affection so that they can later manipulate their lovers-victims into willingly sending them money (FraudWatch International, 2017).

In 2017 Action Fraud recorded 3557 cases of romance fraud which on average equals 10 cases of fraud a day. The report suggests that 63% of victims were women. The actual figures are expected to be much higher given that only a small number of cases come to the attention of Action Fraud due to the embarrassment the victims might feel. Furthermore, it was argued that the amount of £11,500 was lost on average by victims and 18% of the victims were subject to medical treatment due to the victimisation of fraud or major financial losses, leading to possible bankruptcy (Action Fraud, 2018). While a smaller number of victims are affected by romance fraud as opposed to payment related frauds as outlined in the report of Symantec Corporation, the damage per person can be much higher. For example, in one case of romance fraud, a victim lost over £300,000 (Cacciottolo and Rees, 2017).

While the previous reports provided insights into the victimisation of individuals, there are also some statistics and figures on the cost of fraud impacting the private sector. A good source of information is UK Finance (2018) which provides insights into fraud losses affecting the UK payment industry. Fraud the Facts by Financial Fraud Action UK (2017) suggests that in 2017, £731.8 million were lost through unauthorised payments by card, remote transactions as well as payments via cheque. The vast majority (72%) result from card-not-present transactions. Similarly, the Annual Fraud Indicator (AFI) (2017) report by UK Fraud Costs Measurement Committee (UKFCMC) suggests that fraud cost the UK £190 billion from which £140 billion is caused through damage to the private sector.

In addition to committed fraud, the reports on the private sector also draw attention to the attempted fraud cases. A study conducted by ThreatMetrix (2018) – a global security and fraud prevention firm – suggests that in the first quarter of 2018 there were 210 million attempted fraud attacks with an increase of 62% to the previous year. According to the report, the cybercrime attacks largely originate from the USA, the UK, Germany, Vietnam and Brazil. An interesting observation made in the study is

that many attacks are made through bots and not through humans. The report outlines that 1 billion bot attacks were recorded within this period of time, particularly targeting e-commerce businesses. The use of bots in committing digital crimes has also been mentioned in another industrial report, which indicates that bots make up 42% of the traffic on the internet (Distil Networks, 2018).

The multiple sources can lead to a confusing picture, particularly because they only provide partial pictures on cybercrime. The differences can emerge based on the methodological choices and selections made, such as the construction of specific categories, numbers generated through reported offences or crime estimates. For instance, CSEW does not cover fraud against businesses or other government or non-government entities as well as people not resident in households. Similarly, while Cifas and UK Finance provide crime figures on the finance sector, a large number of payment frauds are excluded (Office for National Statistics, 2018). Additionally, the differences can be explained by the varying number and type of cooperation partners involved to create the reports as well as whether reports are generated in the benefit of the public or industrial interests. Industrial reports have further limitations given that different businesses use different names to group cybercrime attacks within a particular geographical area (McGuire and Dowling, 2013) and reports are constructed in a way that will provide an economic advantage to the business; this increases the likelihood of bias.

Another important aspect in relation to the statistics of cybercrime and fraud is that it is often not possible to observe emerging trends as not much comparable data is available. For instance, CSEW only started to include questions on fraud and computer misuse in 2015 while the first AFI report by the UK Fraud Costs Measurement Committee was not published until 2016 (Office for National Statistics, 2018; AFI, 2016). For this reason, it is difficult to find sources showing the true scope and extent of cybercrime (Fraud Advisory Panal, 2016). For instance, Office for National Statistics (2018) suggests that there was a decrease of 15 % in fraud and computer misuse in the UK compared to the previous year while Action Fraud witnessed in 2017 the highest number of recorded fraud offences.

In terms of cybercrime methods, it has been argued that cybercriminals need to break into computer systems or networks, gain access into individual or corporate accounts, and obtain personal or transactional data in order to commit a crime. They can do that either by using technological tools or social skills. For example, cybercriminals use hacking as a method to gain unauthorised access into a computer system or network either to control computers or steal data (Yar, 2013). Additionally, malicious software can be used to facilitate such attacks (Johnson, 2013) which can easily be downloaded by the internet users clicking on an email attachment or visiting an infected website. New malicious software is constantly developed to exploit new vulnerabilities and security gaps (Moore, 2014).

Another popular method used by cybercriminals is phishing which refers to fraudulent emails sent to a large number of people to steal their data. The emails are generated in such a way that they look like they were sent from an official business or financial institution. The internet user is asked to log into their account, for instance to update their details. When the user clicks on the link it redirects them to a fraudulent website. Once the user enters their details the information is sent to cybercriminals who can use the data to take over the user's account to commit identity fraud (Johnson, 2013; Wall, 2007) or sell the data on the dark net.

Social engineering is also a very common method used to commit digital crimes. This method relies on weaknesses in human behaviour. Cybercriminals use social engineering in a social situation to gain access into computers systems, accounts or to obtain personal and transactional data (Johnson, 2013). To do so they need some existing knowledge about their target and use this to achieve their goal (Wall, 2007).

A newly emerging trend is to send a security notice to internet users via email which indicates that some suspicious activity was detected in their bank account, they are then urged to access their account and transfer their funds to a 'safe' account (Financial Fraud Action UK, 2017). Similarly, cybercriminals contact the bank of somebody whose data is compromised and pretend to be the owner of a specific bank account. They claim that they forgot 'their' password and ask the bank to change it so that access can be gained (Schell and Martin, 2004). While cybercriminals need to answer specific security questions to prove that it is 'their' account, they can

also use a Caller ID spoofing service such as Spoofcard. This service makes it possible for the user to select any number they wish to show on the display of the called person. To do so cybercriminals pretend to call from the same number which is registered in the account of the card owner. Such services are also available free of charge (Shavers, 2012). Recent years have furthermore witnessed the emergence of a large number of technical tools which on one hand enable cybercriminals to hide their true locations and identities and on the other hand provide many new opportunities to commit crime. However, one of the most significant developments was the proliferation of cybercrime as a service whereby cybercriminals provide personal and transactional data, technical tools, malicious software and hacking as a service for other cybercriminals. This created a new economy for crime and generated many new opportunities for those who originally lacked technical skills to commit cybercrimes (Shalal, 2017).

Regarding cybercrime offenders, there is only a small amount of information available to provide a comprehensive picture about the background, location and motivation of cybercriminals (McGuire and Dowling, 2013; Levi, et al. 2015). A recent study conducted by Huber and Pospisil (2018) however, provides some insights into the characteristics of offenders. The research of Huber and Pospisil (2018) examines prosecution cases between 2006 and 2016 in Austria to generate a profile of cybercriminals who came to the attention of the criminal justice system within this period of time. They suggest that the vast majority of convicted cybercriminals are male (75%). While it is expected that cybercriminals are highly skilled and have a higher level of education, the study shows that only 8% of cybercriminals possess a degree from higher education and only 5% of cybercriminals are specialised in an IT profession. An interesting finding in this study is that 60% of cybercriminals have an addiction problem which means that the crimes are also committed to support the addiction.

Furthermore, they also argue that 56% of cybercriminals are part of a group, while 41% commit crimes on their own - this means that the majority of cybercriminals do not work alone. However, organised cyber groups do not only consist of people who know each other personally but also people who use the same darknet platforms to

buy or sell cybercrime services. Such platforms enable cybercriminals to develop social ties and to find allies in order to fulfil all necessary requirements to successfully commit a crime (Holt, 2012; Manky, 2013). Additionally, Cifas also provides some insights into cybercrime offending. They argue that more and more young people are turned into cybercrime accomplices. These particularly function as money mules, meaning that they provide their bank account for the movement of illegitimate funds and money laundering (Cifas, 2018).

One of the other main debates emerging from the literature is how law enforcement agencies react to cybercrimes. As pointed out earlier, cybercrimes refer on the one hand to various forms of illegal and deviant activities but on the other hand the area where traditional and new crimes merge beyond any geographical constraints. Consequently, traditional forms of policing are considered insufficient. As Levi et al. (2017) highlight, law enforcement cannot use the same understanding and methods to investigate cybercrimes, given that while crime traditionally is defined within national borders, cybercrimes are carried out within the global and borderless environment (Wall, 2007 /10). Moreover, investigating cybercrimes can be costly and more time-consuming than traditional crimes and exceed the capacities, abilities, knowledge and qualifications of law enforcement agencies (Brenner, 2012; Levi et al., 2017; Leukfeldt, 2017). Furthermore, a common approach is for crime investigation to focus on the crime scene, but in the event of cybercrime, the crime scene can be spread across several jurisdictions, such as the location of the criminal, the victim and any other intermediate locations (Brenner, 2012). Levi et al. (2017, p. 94) add that:

> **Cyberspace has multiple criminal actors living in many jurisdictions whose typologies and methods of organisation and operation do not lend themselves easily to existing definitions and understanding, e.g. in terms of 'hotspots' analysis.**

Consequently, law enforcement cannot respond fully to the complexity and challenges cybercrimes pose. This, however, means that cybercrimes are inevitably neglected and often excluded from statistics (Button and Cross, 2017a), which is perhaps one of the reasons why there are also many other actors who play a crucial

role in “policing” cyberspace beside law enforcement agencies (Grabosky and Smith, 2003). For instance, financial institutions and the e-commerce industry have a key interest in preventing and detecting fraudulent activities – as explored in this research.

The Crime Survey for England and Wales indicates that the victimisation through fraud and computer misuse is 10 times more likely than for instance through theft from the person (Office for National Statistics, 2018). Nevertheless, only 14% of cases are estimated to be reported to the police or other authorities. Low reporting leads to a low number of recorded fraud cases providing only a partial image of the scope and extent of fraud (Office for National Statistics, 2018). Another important aspect is that fraud is still not a priority for local police forces. Since the Fraud Review in 2006, the UK government has responded to fraud offences, for example, by including online fraud in national strategies, launching Fraud Taskforces and Action Fraud. Nevertheless, under-reporting and lack of cooperation between government bodies, law enforcement and the industry make it more challenging to know whether the current measures are adequate and the collected data accurate (Fraud Advisory Panel, 2016; National Audit Office, 2017). Furthermore, while there is an increase in police resources, only 0.27% of police resources are dedicated to fraud/economic crime which are not sufficient. For instance, while benefit fraud makes up only a fraction of fraud/economic crimes, almost four times more resources are dedicated to it (Button et al., 2015).

Even though much effort has been made since the Fraud Review 2006, such as the introduction of The Fraud Act 2006, at this current stage only a few fraud cases are investigated and a very small number lead to prosecution. A key reason for this is that many cybercrimes originate from abroad (Levi, et al. 2015; Fraud Advisory Panel, 2016) which goes along with the lack of reporting. The other issue is that police recorded crimes do not show a clear difference between online and offline offences as offences are recorded under a specific law. This makes the identification of cybercrimes more difficult. While the Computer Misuse Act 1990 covers offences in relation to computer abuse, such as hacking and creation and distribution of malware and others, only a few people were prosecuted under this law (McGuire and Dowling,

2013). In fact, between 2010 and 2015, there were just 169 convictions under the Computer Misuse Act 1990 (Ministry of Justice, 2017). This is additionally because there is no specific law covering all cyber-enabled and cyber-depended offences (McGuire and Dowling, 2013).

The digitalisation of crime raises many questions (Leukfeldt, 2017), the majority of which currently remain unanswered. In the current stage of research, it is often not possible to find clear directions on what constitutes cybercrime or online fraud. The conceptual and definitional difficulties alongside inconsistencies in measuring and reporting create a complex picture, and despite the various understandings and definitions, cybercrimes are often treated as a single but broad phenomenon. Additionally, studies aim to differentiate between traditional forms of offending and those which are committed with advanced technology such as a computer or the Internet. However, treating online and offline separately, or only focusing either technology or human action, is insufficient for understanding cybercrimes, because technologically mediated crimes still have an offline dimension. As Wells (2010) points out, fraudulent activities on the Internet should not be linked solely to electronic devices but rather to people who mobilise them.

Furthermore, the current cybercrime literature gives very little attention to human-machine relations. While there is some acknowledgement that cybercrime needs to be understood in relation to human and technological interaction, as cybercrime is a form of connectivity mediated by the technology that assembles physically remote actors within cyberspace and creates relations, very little information is provided on how such networking is practiced. As Yar (2013) underlines, cybercrimes are the result of social practices which have moved online and opened up opportunities for crime, and so the research can benefit from a more holistic approach. The consideration of the technological and the human and offline sides of online fraud will be crucial to overcoming some of the limitations of contemporary understandings (Leukfeldt, 2017).

An important question that is not posed in the current literature is how we know what constitutes cybercrimes or online fraud, though there is a taken-for-granted understanding of crimes up to a certain level despite the varying definitions or

understandings. While there seems to be common agreement that cybercrimes exist, it is not clear how to differentiate between legitimate digital activity and online fraud. Furthermore, there are also limitations in the current cybercrime and online fraud literature at a theoretical level, given that criminological research is in this field still not theoretically well developed (Leukfeldt et al., 2017). As Aas (2016) argues, criminologists have been very slow to construct theories on how society is technologically mediated or to establish how modern crime control is shaped by science and technology.

This section examined the current state of research conducted on cybercrime and online fraud and laid out everyday realities of cybercrime victimisation. It was argued that while fraud has a long history, new technologies revolutionised its scope and extent on people, businesses and government and non-government institutions (Montague, 2010; Button and Cross, 2017a; Levi et al., 2017). They added a global layer whereby a large number of targets can be easily identified while cybercriminals can remain undetected. Furthermore, a lot of fraud is committed using automated tools (Distil Networks, 2018) which maximise the fraud attempts and minimise the time invested.

Moreover, as previously mentioned, while high rates of victimisation have been addressed through household surveys and corporate sources, this is not reflected in police records, even though the recent reports show a significant increase in reporting (Office for National Statistics, 2018). This is also observed through the low number of prosecutions under the Computer Misuse Act 1990 (Ministry of Justice, 2017). The actual numbers are however unclear because the law does not make a clear difference between online and offline offences (McGuire and Dowling, 2013).

The current responses taken by government bodies are not adequate to tackle the cybercrime problem. This is additionally because the traditional methods of fighting crime do not apply to digital crimes due to their transnational and technical nature (Levi et al., 2017; Wall, 2007 /10). The lack in official response is accompanied by the fact that specific fraud types such as benefit fraud is given much higher priority than digital frauds (Button et al., 2015). This makes the emergence of corporate actors

necessary who are then engaged in other questionable practices while aiming to detect and prevent fraud.

The significant impact of cybercrime on society, in combination with a deficient law enforcement response, has left a complex picture which particularly creates a need for this study. This situation is also reinforced by the current stage of research which does not sufficiently address the complexities of cybercrime dynamics as an assemblage of multiple local, global, individual, governmental and corporate human and non-human actors and also generates a disconnect between the social and the technical while the digital crimes are technologically mediated social practices.

In the following section, social constructionism will be explored as a key theoretical lens that will inform this research and enable to address some of the limitations of contemporary cybercrime literature identified in this section.

2.3. Social Constructionism

2.3.1 The Origin of Social Construction

Social constructionism as a theoretical orientation has been influenced by different schools of thought and intellectual movements (Burr, 2015; Galbin, 2014; Robles, 2012; Hacking, 1999; Holstein and Gubrium, 2008). The term, however, was coined after the influential work "The Social Construction of Reality" by Berger and Luckmann (1966), who suggested that social realities are human constructs, while they may be treated as natural or given.

Berger and Luckmann went on to argue that society is a human product and at the same time humans are the product of their society, which they refer to as an *"ongoing dialectical process"* (p. 149). Humans externalise themselves through a variety of activities and the creation of objects, the latter of which then obtain an independent character or an objective reality. Humans experience these constructions and are affected by them; however, elements in the world appear to be real and objective rather than constructed. As Burr (2015) argues, Berger and

Luckmann show how social realities are created and sustained by individuals based on social practices. While human beings construct the world through their social activities, at the same time it is experienced by them as pre-given. Furthermore, by focusing on the foundation of everyday knowledge, Berger and Luckmann argue that:

> **And in so far as all human 'knowledge' is developed, transmitted and maintained in social situations, the sociology of knowledge must seek to understand the processes by which this is done in such a way that a taken-for-granted 'reality' congeals for the man in the street (p. 15).**

The outstanding argument they make is that knowledge is a process of production rather than discovery, and the sociology of knowledge must examine the ways knowledge is produced. Through their work, they not only aim to challenge the taken-for-granted understandings of knowledge creation, but Berger and Luckmann also encourage social scientists to carry out further research on how scientific and everyday knowledge is constructed. In addition, the literature shows that their work gave rise to many intellectual discussions that tested and expanded the boundaries of social constructionism and sparked an increasingly popular area of research (Burr, 2015; Galbin, 2014; Tänzler and Maras, 2016; Robles, 2012; Potter, 1996; Holstein and Gubrium, 2008).

2.3.2 Contemporary Discussions of Social Construction

Berger and Luckmann's research significantly shaped many contemporary studies, and scholars from diverse backgrounds and different disciplines have explored and adopted constructionist ideas in their studies. As a result of this diverse response, there is little consensus between the contemporary understandings and definitions of social construction(Burr, 2015; Restivo and Croissant, 2018; Stam, 2001; Galbin, 2014; Hosking, 2011; Demeritt, 2002; Edley, 2001; Elder-Vass, 2012; Gergen, 2015; Robles, 2012; Holstein and Gubrium, 2008; Diaz-Leon, 2015; Sveinsdóttir, 2015).

Further, the notion of social construction is used in a variety of different ways (Restivo and Croissant, 2018). For example, while some scholars use it as a label for critical

positions after the influential work of Berger and Luckmann (Stam, 2001), others use this phrase to approach different problems (Hosking, 2011). Although social constructionism is given a variety of different meanings, probably because research has been under the influence of different disciplines as it cuts across a big number of different schools of thought and intellectual movements (Galbin, 2014; Burr, 2015; Gergen, 2015; Edley, 2001), using social constructionism as a label creates confusion (Stam, 2001). The term becomes problematic not only because it is used in different ways, but also because it can refer to conflicting ideas (Elder-Vass, 2012).

Definitional and conceptual difficulties are still prevelent. In particular, social scientists new to this area might struggle with what to call social constructionism, given that it is referred to in a variety of different ways, such as theoretical orientation, movement, concept or position (Stam, 2001). Additionally, discussions surrounding the phenomenon can be found under the label "constructivism" or, more broadly, "postmodernism" (Gergen, 2015), labelling theory or interactionism. Nonetheless, social construction cannot be used as a synonym for these concepts (Restivo and Croissant, 2018; Holstein and Gubrium, 2008); for instance, labelling theory is strongly present in the social construction of crime literature.

Some scholars have aimed to bring more clarity to the diverse and conflicting character of social constructionism. For instance, Gergen (2015) refers to its emergence and current state of as a *"process of dialogue"* that contains not only a particular individual or discipline, but also came into being through a variety of different actors. Due to the vast number of different influences, it can be argued that "*constructionism now belongs to everyone and no one*" (Holstein and Gubrium, 2008, p. 4).

Another way of structuring existing research can be based on their arguments. For instance, Elder-Vass (2012) suggests that we can differentiate between "trivial constructionist arguments", "moderate constructionist arguments" and "radical or extreme constructionism". Although such a classification will bring difficulties regarding where and how to set the boundary, it is useful in terms of assessing constructionist arguments in relation to how studies distance themselves from a given reality.

Social construction as a controversial approach has been criticised by some scholars. A major criticism was posed by Ian Hacking in his study "The Social Construction of What?" Hacking (1999) underlined that the phrase is "obscure and overused". He adds that "*There is no shame in admitting that the term no longer has any meaning (p. 281)."* Other scholars argue similarly by stating that the term has become "dull from overuse" (Demeritt, 2002) or that it has become "notorious" and led to heated debates within "science wars" (Restivo and Croissant, 2018).

Despite its shortcomings, constructionist perspectives have been inspirational for many researchers who do not take social realities for granted. Social constructionism opens up new and creative ways of conducting research (Gergen, 2015), and particularly, researchers are able to engage more critically with science, which claims to be objective, rational, neutral and value-free (Galbin, 2014), while social constructionists acknowledge that any knowledge is developed from a particular perspective and with specific values and preferences. This point will be explored further in the upcoming section on the sociology of scientific knowledge.

Social constructionism as a theoretical orientation is very crucial in understanding what constitutes online fraud. As will be shown throughout this thesis, it is fairly difficult to know in advance whether or not an examined case is actually fraud, because as opposed to traditional crimes, there is not an immediate victim or a clear crime scene which would make online fraud obvious. While some of the cases will "prove" to be fraud afterwards, this is usually too late from the fraud prevention perspective. This means that people aim to detect fraud through automated and manual assessments and stop it before it leads to damage. While doing so, they often rely on their personal views and understandings and make decisions in the hope that these were correct.

Online fraud is a fluid concept, which means that there is often a thin line between what counts as fraud and what is genuine, but equally cases that are labelled as fraud do not remain as such in the future, and vice versa. This implies that a customer can be considered fraudulent today but as genuine two weeks later, while another customer can be considered trustworthy but then categorised as fraudulent after some other transaction occurs. Within this context, social constructionism enables us

to recognise and explore fully the fluidity of and uncertainties surrounding online fraud.

The next section will focus on social interaction as one of the main themes emerging in the literature, which will help to understand how everyday knowledge is produced and maintained and how this affects fraud practices.

2.3.3 The Significance of Social Interaction

Language is a tool necessary to making sense of everyday activities. Humans grow up within particular cultural settings and experience their daily lives through social interaction. Whether it is about how to use a car, how to watch a football game or invite somebody for a coffee, such events become meaningful through language. It is the human interaction and relationships that not only show how daily activities can be managed, but also the meanings attributed to these activities (Berger and Luckmann, 1966; Gergen, 2009). While this view on language has been recognised widely, social constructionism takes a specific stance. Constructionist perspectives suggest that everyday knowledge and common-sense understandings are constructed through the use of language and social interaction (Burr, 2015; Gergen, 2015). Language is not considered merely as a medium through which to express thoughts and feelings but rather as the medium to create a shared understanding (Burr, 2015). This means that when people talk, communicate with others and share ideas, they propose realities. These are then negotiated, maintained and passed on to the next generations (Galbin, 2014; Robles, 2012; Burr, 2015; Gergen, 2015; Witkin, 2011). While with the use of language multiple realities can be proposed and constructed (Witkin, 2011), different constructions lead to different forms of social action or consequences (Burr, 2015). Furthermore, Gergen (2015, p.45) adds that:

> **When we see how language is used to create what we take to be "objective facts", we can begin to question. We can see that these are "facts from a given perspective". We can question the authority of science, policy making, military decision making, economics, and so on. Too often, announcements of "the facts" function to silence other**

> **voices. If you have the facts and I have only "opinions", I am dismissed. Too often the language of objective reality is used to generate hierarchies of inclusion and exclusion.**

As Gergen points out, some realities might find more resonance than others, depending on how the language is deployed. Furthermore, while much of social constructionist writings centre on language as a key element in understanding social realities, Elder-Vass (2012) proposes a certain level of caution about considering this process as a one-way road. He underlines that while language shapes how we understand the world, there is also a physical world that affects how language is constructed. This does not mean that language is not the central point, but it does mean that in addition to language, other human and non-human constructions should also be considered when aiming to explain social realities. Overall, when language is accepted not as something that describes what is out there but rather as something that constructs what is out there, then there is a very different starting point from which to explore those social realities.

A language-based approach is useful in understanding how online fraud is constructed through social interaction between various human actors. While social construction suggests that online fraud is performed from a particular cultural, traditional or historical perspective that is based on values and preferences which may be experienced as natural or real, the language-based approach helps to understand further how fraud is a result of negotiations between different actors. As was previously suggested, while in most cases it is not possible to know factually whether a transaction is fraudulent, actors impose their views and assessments on others during the interaction. Some of these views are then accepted and decisions are made as a result of these negotiations. This will be explored empirically in Chapter Five. This section explored how every day and common-sense understandings are created, negotiated and maintained through language. The next section will follow up by examining how scientific knowledge is constructed.

2.3.4 Social Construction of Scientific Knowledge

The traditional view of scientific inquiry is that science is a process of discovery and enables people to learn about reality (Potter, 1996). Additionally, scientific observations are usually communicated as statistics or facts; however, social constructionism does not entirely agree with this line of thinking and argues that scientific knowledge, in addition to every understanding, can only be "discovered" from a particular perspective (Galbin, 2014; Burr, 2015). This section will explore three major studies, carried out by Latour and Woolgar (1979), MacKenzie (1993) and Knorr-Cetina (1981), to delve deeper into this argument.

One of the most influential works in relation to the social construction of scientific knowledge was conducted by Latour and Woolgar (1979), who carried out their study in a laboratory using discourse analysis while aiming to assess the statements of scientists from a "neutral" outsider position. The core argument emerging from their study was that scientific facts are a result of social interaction and negotiation, arguing that it is not possible to think of scientific inquiry outside the social world, which means that scientists also make choices and selections within the research process, which in turn significantly influence the outcomes of the research. Furthermore, they also draw from their findings that scientists have different ways to interpret research results and are provided with alternative understandings. The statements that turn into "facts," however, are the results of choices as well as social interaction and negotiations. They add that:

> **Our argument is not that facts are not real, nor that they are merely artificial. Our argument is not just that facts are socially constructed. We also wish to show that the process of construction involves the use of certain devices whereby all traces of production are made extremely difficult to detect (p. 176).**

Latour and Woolgar make clear the significance of focusing on the process of constructing scientific knowledge, because when statements are transformed into scientific facts, they are freed from the circumstances within which they were produced. They then become objective observations of reality. Furthermore, another

important point Latour and Woolgar (1979, p. 71) make is that scientists have a key interest in producing results rather than examining methodological issues, because they need to provide publications as "manufactured goods" to be able to maintain their jobs and perhaps receive better positions. This connotes that researchers operate within the constraints of their own social reality and the expectations and requirements posed.

Although Latour and Woolgar take a very critical stance on the traditional understandings of science, they have been criticised for not taking their participants' points of view and scientific discussions into account, as their research explores social interaction in the laboratory without giving voice to scientific content. This critique is in line with the fact that one of the members of the laboratory was awarded the Nobel Prize. Nonetheless, despite this critique, their concept opened up a distinctive perspective for further research that does not take scientific facts for granted (Pinch and Bijker, 1984).

Another influential study on the social construction of scientific knowledge was conducted by MacKenzie (1993), who examined in his work "Inventing Accuracy" how the technological development of nuclear missile guidance systems resulted from the assemblage and negotiations of many actors while drawing comparisons between the United States of America and the Soviet Union. His main claim is that missile accuracy is not a natural consequence of technological developments but *"the product of a complex process of conflict and collaboration between a range of social actors including ambitious, energetic technologists, laboratories and corporations, and political and military leaders and the organisations they head (p. 3).*" MacKenzie aimed to show that the development of a new technology is significantly linked to the social, because while the Soviet Union and the United States were interested in missile accuracy, they had different reasons for focusing on this development. Furthermore, while missile accuracy was important in his research laboratory, other laboratories did not consider it as relevant.

Similarly, Knorr-Cetina (1981) also conducted an ethnographic study, namely "The Manufacture of Knowledge" in the laboratory, by following the tradition of Latour and Woolgar (Potter, 1996). She also claims that scientific facts are socially

constructed, and as opposed to natural things such as rocks, trees or a river, facts are not something solid and are particularly problematic in nature. Moreover, Knorr-Cetina states that facts do not necessarily emerge naturally from observations made but rather they are something that are *"selectively carved out, transformed and constructed from whatever is (p.3)."* Therefore, facts should not be taken for granted, because they come into being through a process of production.

Knorr-Cetina questions further the results produced in laboratories and states that findings are a product of selections and negotiations, starting from the chemicals, tools, methods, validators and publishers with particular interests. She underlines that there is a strong human influence on the choices of the tools scientists use or on the publication of results. In addition to Latour and Woolgar's claim that scientists look for results rather than methodological flaws, Knorr-Cetina observes that laboratory scientists are more interested in making things work rather than pursuing the truth, because the success of a scientific action is more important than finding out the truth.

These three studies can be united under the same critical approach to traditional understanding of science and technology, where findings are linked to observations. However, as outlined in the work of these writers, the development of technologies or facts is highly influenced by human actions, where not only personal preferences and interests are involved, but also where several actors are part of the process. While the production of scientific knowledge involves the engagement, selection and negotiations of different actors, the results are "freed" from these entanglements and represented as "objective" facts and statistics. Furthermore, as Burr (2015) points out, researchers cannot claim they are objective, because research is based on their perspectives and assumptions and it is not possible to move outside of being a human being and observe the world through "neutral" eyes. Furthermore, there is also a historical and cultural context within the research being carried out, and how this occurs is inevitably influenced by the work of early researchers and the cultural aspects. As Potter (1996, p. 10) outlines:

> **Academic writing tends to draw on textual forms – tropes – which construct a god-like, all-seeing, all-knowing, all-comprehending stance,**

> **which is at the same time disinterested and fair. Real authors are, of course, located in history, in particular communities, constrained by their grasp (or lack of grasp) of bodies of ideas, by the quality of their libraries and so on. Writing is full of serendipity and is inseparable from the academic biography.**

This section has provided some crucial insights into how knowledge about science and technology is constructed. This is an important point, as knowing how scientific knowledge is produced helps to understand how online fraud is constructed, particularly how the current research on cybercrime and online fraud builds the foundation of fraud detection practices, while technologies used for fraud detection are taken for granted. It is often assumed that the numbers speak for themselves and are used to distinguish between genuine and fraudulent customers while not taking into account how the scorings come together. The next section takes a similar approach by focusing on actor-network theory, which could perhaps be considered a development of the ideas and perspectives explored in this section whereby the emphasis lies in how multiple actors and non-human entities come together in the making of social realities.

2.3.5 Actor-Network Theory

Actor network theory (ANT) mainly emerged from the sociology of scientific knowledge subfield, particularly from the research of Latour presented in the previous section. As previously explored, work in the laboratory was considered in these early studies as one aspect of the many that were crucial in constructing scientific knowledge. While the collection of heterogeneous actors in the laboratory produced results, these were used to mobilise other actors (Michael, 2016). While these studies marked the beginning of a new and critical approach to science and technology, more studies were conducted and united under actor-network theory (Grint and Woolgar, 1995). Bruno Latour is one of the key scholars, as well as John Law and Michel Callon, strongly associated with the development of ANT (Tatnall, 2001; Fenwick and Edwards, 2012).

Actor-network theory suggests that the world needs to be understood as a relational process – an assemblage of people, things, ideas, organisations, rules and structures – where all of these entities come together to construct social realities. ANT does not consider humans as the only players in this process, as is usually the case with most other theories, and gives non-humans agency while not creating an ontological division between them (Belliger and Krieger, 2016; Law, 2008; Tatnall, 2001; Roberts, 2012). While most sociological theories, for example, use social categories of class or gender to explore social realities, the "flat ontology" proposed by ANT means that there are no hierarchical differences between macro or micro, human or non-human actors. If one actor is considered to be bigger or more important, this is because of the number of their connections and associations and not as a result of a hierarchical relationship (Latour, 2005).

Further, ANT requires a specific language made up of actors and actants, whereby these entities are defined through their associations with other actors (Michael, 2016). Latour (1996, p.7) defines an actant as *"something that acts or to which activity is granted by others*," and it can be anything that is *"the source of an action."* Law (2008: p.141) points out further that:

> **Like other material-semiotic approaches, the actor network approach thus describes the enactment of materially and discursively heterogeneous relations that produce and reshuffle all kinds of actors including objects, subjects, human beings, machines, animals, "nature", ideas, organisations, inequalities, scale and sizes, and geographical arrangements.**

Actor-network theory asserts that society cannot be reduced to the relations of human actors only, since such relations are enabled, transformed and mediated by a variety of non-humans (Nimmo, 2011). This also means that everything in the world is interrelated and entangled. While one can attempt to differentiate between humans and non-humans, from the ANT perspective, such attempts are considered misleading and unproductive (Law, 2008; Law and Callon, 1988; Tatnall, 2001; Nimmo, 2011; Law and Singleton, 2013). As Latour (1992) points out: while there can be differences between human and non-human actors, these are less significant

because ANT does not stress the individual functionality of these actors but rather their cooperation and interaction together and through which the world can be constructed and re-constructed.

ANT's stance on considering humans and non-humans in the same way can easily be misunderstood. For example, Dolwick (2009) underlines that ANT does not aim to propose that all humans and non-humans are equal; instead, they are all interrelated. Even though artefacts cannot think or act as humans do, their physical existence and structure play a significant role. Furthermore, Dolwick (2009, p.38) adds that:

> **It is important to note that within ANT the idea is not to dehumanise humans, or to reduce them to mechanistic forces, but rather to add nonhumans to sociological and anthropological studies.**

Moreover, another key contribution of actor-network theory is how it extends the social to the collective (Latour, 1987). As Latour (2005) points out, the notion of social becomes problematic when it is used to refer to things such as organisational. He aims to redefine what social means by going back to its origin and tracing its connections (2005, p.5):

> **Even though most social scientists would prefer to call 'social' a homogeneous thing, it's perfectly acceptable to designate by the same word a trail of associations between heterogeneous elements. Since in both cases the word retains the same origin—from the Latin root socius—it is possible to remain faithful to the original intuitions of the social sciences by redefining sociology not as the 'science of the social', but as the tracing of associations.**

Similarly, Law (2008) emphasises that the social cannot be studied without taking its relational materiality into account. While this can sometimes be viewed as turning away from the social, Law emphasises that many sociologists fail to see how it is held together. He differentiates between a material and non-material form of the social and points out that sociologists often focus on the non-material form and ignore the notion that the social is generated through material practices. As ANT understands

the world in terms of heterogeneous networks of people and things, the social can therefore not be attributed purely to humans – it is shaped by the various networks that are a part thereof. As an example, human interactions are mediated through objects, such as text and computers (Law, 1992).

Moreover, the heterogeneous network serves as a metaphor to illustrate one of the main ideas of ANT, in that society and other entities are the effect of diverse and unstable relations (Law, 1992) which are made and remade and are kept alive through this process of making and remaking. Stability can be achieved as long as this interaction continues; for example, a business department can only exist when employees continue to go to work (Dankert, 2011). Furthermore, the generation of new connections and networks is performed through so-called "translation" (Law, 1992), which means that actors are enrolled into actor-networks by other actors when they or their interests are shifted through negotiations, calculations or representations such as scientific papers (Dankert, 2011). The medium of translation is intermediaries. As Michael (2016) points out, the relationship between humans and non-humans requires the circulation of artefacts, objects and people to translate actors. Furthermore, the strength of actor-networks results from their associations (Callon 1998; Dolwick, 2009), which emerge when actors are enrolled and translated into networks (Belliger and Krieger, 2016). From this ANT perspective, power depends on the extent or the quantity of associations of actors (Michael, 2016; Dolwick, 2009).

Actor-network theory can be considered a constructionist theory, while ANT proposes a more radical form of constructionism (Michael, 2016) by bringing non-humans into play. Additionally, as Dankert (2011) points out, the emphasis on connections between actors illustrates that the ways they are connected and reconnected with each other lead to a variety of different realities. This also becomes clear in ANT's notion of the multiplicity of realities that are performed in practice (Mol, 1999).

However, ANT has often been criticised in two major ways. First, as Law (2008) outlines, theories normally look at causes, while ANT provides a descriptive account

of relations in a network and enables researchers to unravel relations. For this reason, ANT has been challenged as to whether it is actually a theory. Law (2008) suggests that it would be better to consider it an approach, while Callon (1998, p. 194) adds that they "never claimed to create a theory", outlining that ANT aims to provide researchers with an analytical tool for situations where it may not be easy to distinguish between humans and non-humans, because human action cannot be attributed purely to humans but also involves non-humans. Thus, human action can only be extended by the recognition of non-humans in different forms and various networks. Secondly, ANT has been criticised for proposing a symmetrical relationship between humans and non-humans, though Callon (1998) points out that this is also one of its main strengths.

In relation to online fraud, ANT provides a theoretical framework through which to explore fraud as a relational effect of multiple actors embedded in heterogeneous and multiple networks. In addition, it emphasises how humans and non-humans are inseparable and how human action is mediated by non-humans. Online fraud inevitably entails a number of humans and non-human actants such as technology, organisations, working environments, roles and responsibilities, hierarchies and external pressures. ANT suggests that we can only fully explore online fraud by "following the actors" (Latour, 2005, p. 12) and the traces they leave. Furthermore, Dolwick (2009) points out that the ANT perspective on the social provides a broader understanding by viewing it as a series of associations between all possible actors, nature, humans and material artefacts. When the social is not attributed to humans but is an assemblage, this raises the question as to how actors might connect, disconnect and reconnect again to other actors. Understanding online fraud management as an assemblage of interconnected actors provides a good starting point from which to unravel these connections.

Furthermore, ANT is also helpful in understanding the role of organisations and workplace culture in fraud constructions. Organisations can be considered as social systems consisting of technological and social components whereby all parts of the organisation are linked to each other and influence one another (Fox, 2007; Belliger and Krieger, 2016). While organisations may appear as entities with boundaries and

clearly defined rules, they are considered as activity negotiating and building actor-networks and making temporary associations with a variety of different human and non-human actors (Grint, 2005; Belliger and Krieger, 2016). As Nimmo (2011) outlines, organisations do not only entail human relations, since such relations are enabled, transformed and mediated by a variety of non-humans.

Moreover, organisations are also social constructs with varying structure, ideology, and culture of management which means that the way organisations are structured has a major impact on how employees work, communicate with their co-workers, behave, make decisions and perform tasks using existing technological tools and systems (Fox, 2007; Volti, 2011; Grint, 2005). As it will be discussed in Chapter Six, the workplace has a significant impact on how online fraud is constructed. Particularly as organisations consist of temporal associations, the way organisational actors come together and build associations leads to the generation of different forms of online fraud.

This section identified and critically discussed the key elements of social constructionism, proposing that with the addition of actor-network theory a more holistic approach can be taken where not only human but also non-human actors are considered. This provides a strong theoretical framework to explore technologically mediated online fraud.

2.4 Social Construction of Crime

After exploring key constructionist ideas, this section shifts attention to crime and examine how it can be explored from constructionist perspectives. The aim is to critically assess how crime is considered a social construct in the contemporary literature, identify strengths and shortcomings and demonstrate to what extent this research will depart from these established approaches and then examine how including big data as an assemblage of non-human actors helps overcome some of the identified limitations of current perspectives.

2.4.1 Constructionist Perspectives on Crime

Crime as a social construct is not a new concept and has been widely recognised by many scholars within the sociological and criminological literature (Polizzi, 2016; Henry, 2009; Rosenfeld, 2010; Czabanski, 2008; Becker, 2008; Eglin and Hester, 2013; Christie, 2004). The social construction of crime emerged from theoretical perspectives such as labelling theory, symbolic interactionism, postmodernism (Barak, 2013; Rafter and Brown, 2011). Many scholars from varying disciplines contributed to social construction even though their ideas were not explicitly expressed using the label of social construction. For instance, the labelling theorist Becker (2008) did not claim to be a social constructionist, but his arguments contribute to constructionist perspectives on crime (Rosenfeld, 2010).

Social construction is a distinct approach that challenges the everyday assumptions and realities of crime and criminal behaviour – as opposed to traditional criminology, which often aims to explain the risks and causes of crime (Kirwan and Power, 2013). Furthermore, crime is typically linked to young, male and unemployed individuals in society who are from low socio-economic backgrounds (Burke, 2013). Such approaches often rely on a statistical understanding of crime which social constructionists usually oppose, because it implies that crime is a self-evident phenomenon in society (Muncie and McLaughlin, 2001). As Becker (2008) underlines, this statistical understanding focuses on deviations from the norm. As we shall see in the following chapters, the contemporary methods of fraud detection make use of such assumptions that rely on the characteristics of fraudsters and non-fraudsters. By using statistical methods, people who deviate from the norm are suspected of being fraudsters, but by also focusing on characteristics such as income and social background, fraud detection makes use of traditional assumptions qua criminality. Another important point raised by Becker is that traditional theories of crime focus on the why question, for instance, why did somebody commit a crime? Why do people commit online fraud? However, social constructionism asks how something has come into being and not why something has happened.

As highlighted above, the social construction of crime has come under the influence of different disciplines. A social constructionist account of crime emerging from

labelling theory sees the causes for its existence merely attached to certain acts. Crime does not exist as an objective fact; it is a label and the meaning we give to certain acts (Treadwell, 2012; Ugwudike, 2015; Czabanski, 2008; Muncie and McLaughlin, 2001). Once society has successfully attached such meanings, then these acts become crimes (Christie, 2004; Polizzi, 2016). In Becker's view, social groups create rules about right and wrong and take great interest in enforcing them, and once these rules are created, some of these individuals turn into rule breakers, thus making them untrustworthy and ‘‘outsiders’’. However, the rightness or wrongness that people attribute to acts change over time, even though the act might remain the same (Rosenfeld, 2010). This shows that crime is historically and culturally variable, and although there can be some overlap between societies' definitions and understandings of crime, there are still many differences; for instance, some human actions in the past were not considered criminal but are now considered as such. As an example, until the 20th century white collar and corporate criminals were rarely punished because these crimes were not labelled as real crimes despite the significant cost, they generated (Henry, 2009).

Becker's labelling perspective on crime is a useful concept as it gives insights into a variety of possible constructions of crime. For instance, Becker highlighted that society decides about right and wrong behaviour through existing norms and values. Given that societies are very diverse, the understanding and conceptualisation of crime will be diverse, too. In relation to online fraud, this perspective helps to understand how it has now become an accepted and problematic form of crime, in particular within industrialised countries. Labelling theory explains why online fraudsters are labelled as criminals, in that they represent a threat to existing structures, norms, and values. Nevertheless, labelling is more concerned with how particular acts, for instance illegally obtaining the payment details of others, becomes online fraud rather than focusing on social relationships and communication, which are more central to the ideas of social constructionism.

Furthermore, many social constructionist writings centre on the adaptation to and enforcement of laws, given that crime can only exist when acts are defined as such through the construction thereof. Many unwanted acts can then be turned into

crimes through the labels attached to them, which, however, also undergo a process of negotiation between the rule breaker and law enforcement actors (Eglin and Hester, 2013; Czabanski, 2008; Christie, 2004). Crime exists through the definitions given by individuals such as law enforcement officers and politicians that have the power and authority to create laws against individuals who threaten their interests (Henry, 2009; Ugwudike, 2015; Treadwell, 2012).

The social constructionist critique of traditional perspectives on crime has been highlighted before, particularly in terms of targeting lower-class criminality. However, the main evaluation posed here is not that the moral quality of the act makes it criminal but rather the social and legal responses to the act. Consequently, it is not the harm or impact of the act that makes it a crime but often the social and moral status of both the offender and the victim (Rosenfeld, 2010; Ugwudike, 2015; Treadwell, 2012; Becker, 2008). Furthermore, power inequalities can be enforced through the supporters of particular groups within society, while such inequalities appear to be normal or natural (Burr, 2015).

The constructionist literature on law enforcement embodies aspects of labelling and power relations. In terms of online fraud, there is a similar relationship between those individuals who have the power to label and those who receive the label of online fraudster. Although this research considers power relationships as an important aspect of the construction of online fraud, it does not entirely agree with the argument that whether or not an offender will be punished depends on his or her social status. From an online fraud perspective, often cost-benefit aspects are more important, which will be explored in Chapter Seven.

This section showed that there are some limited studies on exploring crime from a constructionist perspective. In relation to online fraud, there seems nevertheless to be a lack of research so that this study can build on existing literature of crime. These critical studies are beneficial because they move away from the traditional understanding of criminal behaviour and provide an alternative perspective. In particular, understanding the variability of crime, culturally and historically, and the critique of the statistical methods of crime detection and prevention and traditional profiling can help to question the taken-for-granted understanding of crime.

Furthermore, crime as a human construct also implies that this social reality is subject to social change, social biases and prejudices within existing structures, so these aspects also need to be taken into account.

Nevertheless, the existing constructionist literature on crime only provides limited support for this research. Particularly, the predominant labelling perspective focuses on face-to-face interactions and not on the form of the technologically mediated connectivity proposed in the study of online fraud. Furthermore, while crime is defined through the labels attached by human actors to others, this research takes a holistic approach by looking at crime as the result of human and non-human relations and entanglements, because digital crimes cannot be fully explained through social factors alone or through digital technologies.

There have been some efforts to combine human factors and technology in cybercrime research, particularly through the lens of ANT. For example, Luppicini (2014) conducted extensive research on how ANT was applied in cybercrime research by analysing research papers from 2002 until 2013, identifying that it was used by some researchers within cyber criminology to develop an understanding between human and technological relations. In addition, ANT provides a theoretical lens for cybercrime-related studies by recognising the complexity of human and non-human interactions without having to decide on micro or macro levels of network relations. Moreover, it has begun to be used gradually in cybercrime research by providing researchers with a theoretical framework to explore the complexities of technologically mediated cybercrimes. Luppicini (2014) emphasises that there is a clear theoretical gap in addressing the complexities of cybercrime involving humans and technology, since very little space has been given to theory within cybercrime-related studies.

At the beginning of this study, the theoretical orientations, rational choice and routine activity theory were also taken into consideration. The rational choice theory considers criminal behaviour as a rational calculation (Cornish and Clarke, 2014) whereby criminals make a subjective cost and benefit assessment. Criminals compare the likely gain generated through the criminal act with the possible costs such as penalties in the case of detection. If they feel that the benefits outweigh the costs, they decide to commit the crime. However, while the theory implies that crime is a

rational decision, it proposes only partial rationality. This is because all choices and decisions are made with limited available information, existing influences and constraints (Akers, 2013; Cote, 2002; Eriksson, 2011).Furthermore, the rational choice theory suggests that people with particular individual and dispositional traits such as low self-control, selfishness and a pleasure-seeking attitude are more likely to commit crime (Piquero and Tibbetts, 2001; Cote, 2002). The rational choice theory is a situational crime assessment and focuses on the situational context when the decision-making takes place (Cote, 2002; Cornish and Clarke, 2014; Clarke and Felson, 2004). This approach is used to explain both traditional and digital crimes (Leukfeldt, 2017; Yar, 2016; Bossler and Holt, 2009).

The routine activity theory suggests that a criminal act requires motivated offenders, suitable targets and the absence of capable guardians. While the presence of one or more of these elements reduces crime, the lack of capable guardians significantly increases criminal rates (Cohen and Felson, 1979). The routine activity theory was developed to respond to changes in routine activities after the Second World War which created an easier access to potential targets (Akers, 2013; Clarke and Felson, 2004). This theory has increasingly been applied to the areas of cybercrime, such as malware intrusion and infection, phishing, insider cybercrime and cybercrime offending (e. g. Hutchings and Hayes, 2010; Bock et. al, 2018; Kigerl, 2012; Bossler and Holt, 2009). For instance, Hutchings and Hayes (2010) looked into the victimisation through phishing. They argue that routine activities of individuals have created new targets for fraudsters. While email filters serve as guardians, they are not able to detect all phishing emails.

Both theories were disregarded because this research does not examine the individual traits and motivations of cybercriminals or how technological developments generated new routine activities which open doors to crime. This research rather challenges taken-for-granted understandings on what constitutes a crime and examines how people, technology and data come together in the making of online fraud. It also aims to expand upon the existing literature by particularly looking at the social practices, actor-networks, assemblages and entanglements of humans and non-humans constructing online fraud. Thus, given the focus of this

research, both rational choice and routine activity theory were not considered as an adequate theoretical framework.

The next section will look at big data as one of the key non-human assemblages, in order to expand upon the understandings generated in this chapter and to explore the final piece in this study, which plays a crucial role in the construction of online fraud.

2.4.2 The Role of Big Data in Fraud Construction

This section explores data as a specific assemblage of non-humans that represents the basis of fraud practices. Fraud management relies on generated and collected datasets that are accessed and used for fraud categorisations and scorings. From the fraud management perspective, fortunately, there is a significant amount of data generated through daily online activities. For instance, visiting webpages, liking and disliking, sharing videos or photos, pages, emails and text messages all leave digital traces (Neef, 2014). While people make use of the Internet and new digital devices to manage their daily lives, online traces enable others to record and watch their decisions (Payton and Claypoole, 2014). In relation to online shopping, for example, online retailers can track digital activities to check products customers have viewed, purchased items, visited pages and the amount of time spent viewing and purchasing products. Online purchasing generates data on both usage and transactions that are tracked, simplified, analysed and reported (Ruppert et al., 2013), at which point millions of "facts" about consumers are collected (Payton and Claypoole, 2014), including their personal information (Bunnik et al., 2016) and transactional data for surveillance and control (Payton and Claypoole, 2014).

Organisations in particular increasingly perform routine surveillance practices against individuals, customers, other groups of people and the population at large (Lyon, 2014; Stoddart, 2014). One of the key actors performing mass surveillance techniques and practices are corporations. Corporate surveillance entails collection and use of data for economic purposes (Leckner, 2018). In fact, digital data has led to

the emergence of new business models and it has become a main asset for organisations and businesses to gain a competitive advantage over others. Business objectives are achieved through generation, analyses and classification of data (Esposti, 2014). Mass dataveillance has become a normalised practice amongst corporations to make automated and data-driven decisions (Christl, 2017).

Lyon (2003) uses the phrase "social sorting" to describe how computer code, automated screening, identification techniques, and personal and transactional data, as key features of everyday surveillance, are used to generate social and economic categories for individuals. He builds this notion on Oscar Gandy's "panoptic sort". The work of Gandy focuses similarly – within the context of marketing – on how customers' personal information is used to identify, classify, assess and then sort individuals into categories of economic value (Gandy, 1996, p.135). Gandy (1996) argues:

> **The collection and use of personal information are critical to the operation of what I have called the *panoptic sort*. The panoptic sort is a complex discriminatory technology. It is panoptic in that it considers *all* information about individual status and behaviour to be potentially useful in the production of intelligence about a person's economic value. It is a discriminatory technology because it is used to sort people into categories based upon these estimates (p. 133).**

Gandy suggests that personal information is essential to identifying individuals and differentiating them from one another. For companies, it is crucial to know their business partners, for instance when they are providing goods and services. Gandy's point, however, is that identification is used not only as evidence that people are really who they say they are, but also to generate customer records, to divide them into groups based on the same attributes and characteristics, with the outcome of valuing some and discriminating against others.

To Gandy, while such classification models decrease the level of uncertainty experienced by businesses and help them estimate the economic value of people, and whether they are worth targeting for economic reasons (for example, whether individuals should be sent specific adverts), the classification models are simplifications, as they reduce individuals to a small number of attributes while not

considering the complexity and uniqueness of human nature. Gandy argues that once individuals are identified and divided into categories, the assessment determines whether customers are included in or excluded from marketing practices.

Lyon's (2003) understanding of surveillance goes beyond Gandy's panoptic sort, whereby surveillance is performed by those with power over others. To Lyon, surveillance is an everyday and democratised practice, as technological developments make it possible for everybody to monitor and track human behaviour. In addition, Lyon (2005) argues that the disappearance of bodies represents the basis of surveillance practice, given that individuals perform their daily activities at a distance. Individuals' abstracted digital data doubles are collected and reassembled in remote locations for sorting (Haggerty and Ericson, 2000).

Lyon (2003) suggests that the key features of social sorting are the collection of personally identifiable data, accessed through the use of "remote searchable databases" (p.2). Remote access to rich sources of data provides the opportunity to differentiate between individuals and sort them into risk categories; however, the constructed categories of people can also be re-constructed in different ways, based on whether risk categories are accepted by those who are subject to these surveillance practices. Lyon (2003) points out:

> **Risk management, we are reminded, is an increasingly important spur to surveillance. But its categories are constructed in socio-technical systems by human agents and software protocols and are subject to revision, or even removal. And their operation depends in part on the ways that surveillance is accepted, negotiated, or resisted by those whose data is being processed (p. 8).**

Similar to Gandy, Lyon (2003) argues that while human life inevitably requires the generation of categories such as children, adults, citizens, employees and so on, the categorisation of individuals is rationalised and automatised though surveillance practices whereby richer sources of data are handled in a speedy manner and different sources of data are drawn together, often without the knowledge of individuals, for risk assessments.

For instance, when engaged in digital activities, people are often unaware what additional data have been disclosed, such as IP addresses, device details, etc. (Lyon, 2014). When users visit a website, hidden software codes can capture data about their digital behaviour, how they click, scroll, touch and navigate through the website and then how they store these data (Christl, 2017). Additionally, while social media enables individuals to engage with people such as family members or friends, data companies also collect a lot of information about the user at the same time. All of the different types of data collected through different sources can then be used together for social sorting. According to Lyon (2003), while surveillance based on the use of technological tools and personal data emerges from the need to deal with the changing lifestyles of a population with increased mobility, as well as challenges emerging from the disappearance of bodies, surveillance technologies entail stereotypes and prejudices and affect the life chances of those who are subject to such scrutiny.

These surveillance practices are not only performed for fraud detection and prevention but also in other contexts such as in credit and loan applications, during the recruitment process or at the airport. For instance, social sorting is used in the assessment of credit and loan applications and in the generation of credit scoring models in order to determine which people will be granted a credit and which will not. This has however serious financial implications because this process results in either receiving a credit or not being eligible affecting their current and future situation (Ball, 2019). Similarly, a common practice in the recruitment process is the examination of 'data doubles' of jobseekers for background checks who will not know which parts of their privacy might have been shared with the possible employers. This practice influences whether an applicant will be recruited (Hedenus and Backman, 2017). Furthermore, Herlyn (2014) argues that passengers at airports are subject to social sorting practices. Passengers are managed and sorted based on their characteristics and without their knowledge whereby social and cultural categories are generated leading to varying treatments of people.

Everyday surveillance practices divide people into groups with long term consequences given that some are assigned worth and granted access into particular

aspects of life whereas others are not. Social sorting results from social arrangements and information technologies whereby categories of people are constructed and normalised (Herlyn, 2014). Furthermore, merging different sources of data into one or grouping various fields of data also means that data can be connected and re-connected in multiple ways (Van der Schyff et al., 2018; Stoddart, 2014).

Additionally, these practices are problematic also because they are performed without the knowledge or consent of the participants (Strong, 2015; Kitchin, 2014a; Lyon, 2006). People have only limited control over how their lives are increasingly "datafied" for classifications and fraud detection purposes. Furthermore, these data are often repurposed and used in ways which were not for the intended usage when they were generated (Kitchin, 2014a). For instance, details generated through order placement are used not only to process and deliver an order, but also to categorise customers and make judgements about them. As will be explored in Chapters Four and Five, this process goes beyond the usage of data generated in the transaction only and looks for additional information on the Web, while customers are often not aware of these practices and have no control over them. Nevertheless, placing an order online requires compliance with this approach; otherwise, it is not possible to make an online purchase. For example, if there are no digitally accessible data about customers which will confirm that they are who they claim to be in their order details, then it is likely that they will be considered suspicious.

Another main problem with data is that they are not neutral representations of reality. The digital collection of data leads to specific assemblages of people (Lupton, 2014) that are used to construct scoring systems and predictive models which also entail human selections and biases (Pasquale, 2015). The choices humans make reflect their own value. Furthermore, selections are made to decide what is important enough to include, while other aspects are excluded (O'Neil, 2016). Additionally, it is misleading to assume that the "numbers speak for themselves" (boyd and Crawford, 2012, p. 666), given that they need to be considered by taking into consideration human biases that prevail in the collection and analysis of data; otherwise, there is the risk of misunderstanding data outcomes (Crawford, 2013).

In addition to the selections humans make, it also needs to be understood that datasets are not perfect and can indeed contain errors and inconsistencies (Kitchin, 2014a), including gaps. However, these unreliable data still can be used for constructing other datasets. As a consequence, patterns can be extracted from non-existent or incorrect data (boyd and Crawford, 2012). Furthermore, data are not able to display completely the complexity of the real world and human interactions. Digital systems are a simplification of the world from which facts are created (O'Neil, 2016). To reduce human behaviour to data points lacks recognition of the context and the complexity of human behaviour (Strong, 2015).

Nevertheless, it is important to acknowledge that big data represents new methods of creating social knowledge (Burrows and Savage, 2014), reconstructs ways of acquiring knowledge and offers new methods of defining and categorising information on our social reality (boyd and Crawford, 2012). However, data-driven knowledge does not necessarily differ from traditional scientific knowledge in its limitations – as outlined previously. For instance, boyd and Crawford (2012) argue that big data as a method of conducting quantitative research is not necessarily a better way of achieving an objective truth. Additionally, it aims to present theory-free scientific knowledge (Kitchin, 2014a), but datasets cannot be theory-free when aiming to discover patterns, especially given that researchers need to engage actively with these data and interpret them from their own perspectives (Crawford at el., 2014). Thus, claims to objectivity are based on subjective preferences, choices and observation (boyd and Crawford, 2012).

Even though big data can create patterns and relationships, the relevance and significance of these patterns are based on questions asked to the people (Andrejevic, 2014). As an example, crime detection and prevention in line with big data have received significant attention over recent years, and in particular how social media could be used to predict future crimes. For instance, Twitter provides publicly accessible data whereby different pieces of information are combined to generate correlations between social media content and criminal behaviour, for instance to examine whether an increase or decrease in crime rates can be predicted (Aghababaei and Makrehchi, 2016).

Knowing that big data is unstructured, noisy and messy (Williams et al., 2016), and can include meaningless content (Atefeh and Khreich, 2015), choices and selections must be made to deal with it accordingly. Furthermore, data can give the impression that they are transparent and provide access to the truth; however, when speaking of data, words such as ‘‘collected,’’ ‘‘entered,’’ ‘‘compiled,’’ ‘‘stored,’’ ‘‘processed,’’ ‘‘mined’’ and ‘‘interpreted’’ are used to describe the procedure behind this process (Gitelman, 2013, p. 3), which limits the objectivity claims of big data.

A critical perspective on data in relation to online fraud requires scrutiny of its position as a neutral method of representing social reality. As this section has shown, there are significant limitations to the claimed neutral position or being the representative of an objective reality, because all knowledge must be considered within a historical or a cultural context, influenced by individual choices, values and preferences. This is important to note, because the end product will be freed from influential aspects within the construction process. For this reason, it is crucial to explore how datasets are constructed and how they relate to the construction of fraud practices. Furthermore, as will be examined in Chapter Four, data create a form of connectivity that is neither neutral nor given. How data are generated and assembled is crucial to understand, because they lead to specific constructions of customer profiles and black box scorings, which are then used for manual fraud assessment.

This chapter explored the key ideas behind social constructionism and actor-network theory in relation to online fraud. It proposed that by considering both theories a better understanding can be generated which can respond to the complexities and entanglements of online fraud. The social constructionist perspective helped to challenge the taken-for-granted understanding of online fraud that accepts it as something given rather than constructed. In addition, the chapter drew on the notion of knowing and underlined that knowledge can only be generated from a given perspective, understanding, set of values and preferences. The notion of knowing is fairly complex in online fraud, because, as will be explored in Chapters Four and Five, knowing in advance which cases are fraudulent is often not possible. A transaction becomes fraud as a result of social practices. This understanding was developed by

the application of a language-based approach, which will be empirically explored in Chapter Five. It will be shown how fraud realities are proposed and negotiated, accepted or rejected.

The section on the social construction of scientific knowledge suggested that all forms of knowledge, including scientific facts, are a process of production. This is a useful perspective from which to explore the developments of current fraud management systems and their outcomes as numbers and scorings. While fraud scorings can be the result of selections, calculations and negotiations, these become an objective reality for those who employ them. As will be demonstrated in Chapter Four, fraud scorings not only create clear distinctions between genuine and fraudulent customers, but they also influence how agents manually assess and categorise them.

A strong theoretical framework has been provided in two ways through the inclusion of actor-network theory. First, as the notion of social is extended to non-human actors, the role of heterogeneous actors in the making of online fraud will be made visible throughout the empirical chapters. Chapter Four will explore how social practices are mediated by technology and data, and Chapter Five will illustrate that decision-making involves technological developments such as the Internet, Google Search, geographical data and telecommunication. Chapter Six will examine how fraud is partly the result of several human and non-human actors entangled in organisational relations, and Chapter Seven will assess how these relations can be extended to other actor-networks.

Second, as will be explored in Chapter Three, the methodological application of ANT opposes any form of separation or dualism, such as micro and macro or online and offline, and extends the possibilities of exploring any form of interrelation by following the actors. Online fraud can be characterised through entanglements of practices that are performed in cyberspace and within a physical space such as an organisation. Thus, online and offline dualism is not useful, while such entanglements can move beyond the immediate environment. As Wells (2010) points out, internet fraud should not be linked solely to electronic machines but rather to the people who mobilise them.

Additionally, the section on the role of big data analysed how fraud practices are grounded in data, which are far from being a neutral or an inevitable way of creating relations for manual assessments. The next section will provide a brief overview of the insights gained from the literature, before detailing the research questions.

2.5 Conclusions and Research Questions

In light of the reviewed literature in relation to social constructionism, actor-network theory, crime-related studies and big data, it can be argued that the literature only provides limited understandings on online fraud while online fraud as a concept is taken for granted. This research aims to address this gap by taking a constructionist approach and extending the notion of the social to non-humans, in order to offer a more holistic approach to fraud. Through insights gained from the literature provided in this chapter, this research will critically explore how online fraud is socially constructed. By focusing on the fraud management practices of several online retailers, this research centres on the following question:

- How is online fraud constructed through social practices and technological and organisational relations?

The sub-questions are:

- How are online customers categorised through their data?

- How is online fraud constructed through social practices?

- How can online fraud be understood as a relational effect?

- How do external actor-networks relate to fraud constructions?

This study aims to critically engage with automated and manual fraud management and provide a unique insider perspective on how fraud constructions are performed. It also aims to analyse the limitations of fraud prevention and detection methods and show the social and ethical implications for the wider public.

3. Methodology

3.1 Introduction

The previous chapter critically examined the contemporary literature on cybercrime and crime-related studies and identified that there is only limited research available on online fraud, particularly from a constructionist perspective, which not only takes into account human actors, but also considers how cybercrimes are technologically mediated. The chapter proposed that research can certainly benefit from taking a holistic approach by considering the combination of human and non-human actors in the perpetration of online fraud. This chapter details the methodological approach taken to address the focus of this research.

Any research problem can be addressed by taking different methodological paths. Within the social sciences, as Silverman (2015) points out, research can be conducted by taking a positivist, naturalist or constructionist approach. While positivists aim to "discover" social realities regardless of the role of the researcher or participant, naturalists are more interested in meanings and shared understandings. As explored in Chapter Two, constructionists take a different approach and claim that scientific knowledge is a process of production rather than discovery while focusing on common-sense understandings and practices. The constructionist perspective provides the researcher with a unique position to go beyond the obvious and dig deeper by looking at how something comes into being in otherwise taken-for-granted practices.

Furthermore, another important point that constructionism makes is that the researcher needs to be aware of their position within the research process, i.e. they are not a "neutral" observer outside of the research process (Gibbs, 2008) but an active participant in generating research findings. For this reason, while making a rigorous examination of the selected research design, it is also crucial as a critical researcher to recognise how one may influence the research and consequently the outcome of the study. This means that transparency should be provided on how the relationship between the researcher and the researched is a key element while reflecting on the research methods and design (Flick, 2014).

Moreover, Tanner (2008) observes that it is impossible to conduct a value-free study when generating scientific knowledge, because researchers have personal characteristics, varying biographies, backgrounds, social influences, preferences and interests – each of which will influence or limit their understanding, observations and interpretations. Thus, the individuality of the researcher should also be taken into account when approaching the fieldwork. Tanner (2008, p. 36) adds that:

> **No fieldworker has ever approached their research in a neutral and scientific frame of mind.**

While scientific studies are often based on claims of neutrality or objectivity, it is impossible to move outside of being humans and see the world through "neutral" eyes (Burr, 2015), because the type of neutrality expected by scientists does not exist, as explored in the previous chapter. The best thing the researcher can do, therefore, is to accept that their background inevitably influences how a research problem is approached and to reflect on this appropriately. Most importantly, one should be aware that this relates not only to the research of *others*, but also to one's own work.

Keeping this in mind, this chapter will explore a number of relevant methodological issues while leaning towards a constructionist perspective, with the aim of being self-reflexive and critical of the research process, design, methods and so on. The chapter is divided into four sections. The first section discusses the key elements of doing insider research, as this study was conducted during my employment in a customer service centre in Germany. It is examined how being an insider was the most crucial factor that not only created interest in choosing this area of research, but also gave rise to how it was designed and conducted. However, being an insider also creates challenges for the researcher so that it is discussed in the section how these challenges were addressed accordingly. The second section assesses the choice of research methods. This research uses a mixed method approach of semi-structured interviews and auto-ethnography, which were selected in conjunction with being an insider and as a scholarly justification for addressing the gap in the literature. This is because the qualitative approach enables one to go deeper into the daily experiences and practices of a variety of actors and to look into how practices come into being.

With the additional insider perspective, more breadth and depth could be achieved. The third section addresses the data collection and analysis process by discussing the data collection methods and how these data were coded and analysed. In the final section, a critical discussion of the ethical issues of conducting qualitative and insider research is provided, and it is outlined which steps were taken to address these problems.

3.2 Being an Insider Researcher

Chapter One noted that the choice to focus on online fraud as an area of research started with early observations at the customer service centre, where fraud was managed amongst other customer-related duties on a daily basis. Perhaps the most interesting observation amongst them was the normality of fraud in a legitimate company and its acceptance as just being part of the business, like any other legal practice. This was followed up by the observation of how agents at the customer service centre made individual fraud assessments, not only because they varied in their understanding of fraud and who they suspected as possible fraudsters, but also how these practices were taken for granted, maintained and passed on to newcomers without much consideration. While this was certainly a very stimulating experience, it made me at the same time wonder why I had not come across such fraud practices while having previously engaged with the academic literature on business and cybercrimes.

This was a good starting point for me to look for ways to explore fraud at the customer service centre. When I actively sought to be involved more strongly in related tasks, to gain a deeper understanding, I was offered an additional position in the fraud management of a major online retailer. While early observations triggered my interest in choosing fraud as an area of research, the subsequent – and more active – engagement with a variety of related issues was more crucial in developing a deeper understanding of prevention and associated management systems, methods and practices. This in turn formed the nucleus of becoming an insider researcher.

This has been a flourishing journey, because being an insider not only enabled me to recognise the significance and everyday experiences of online fraud that were not sufficiently addressed in the academic literature, but it also gave me the opportunity to develop technical knowledge on the subject, to gain access to the site and participants and influenced the depth of data that I was able to collect. As Costley et al. (2010) note, being an insider provides the researcher with a unique opportunity to focus on a research problem while making use of their insider knowledge and experiences as a solid foundation on which they can build (Bailey, 2007). Furthermore, Bailey (2007, p. 38) highlights that:

> **Those who are familiar with a setting may already have rapport with participants, understand the nuances of language and behavioural expectation and possess analytic insights into the working of the setting.**

In addition, again according to Bailey (2007), being an insider creates familiarity with the structures and issues within a particular setting (Galletta, 2013), but also it provides the researcher with the repertoires that an outsider is not able to understand. This gives the insider researcher an advantage, in that he or she can develop a deeper understanding not only of participants' life experiences, but also of the conditions within which these experiences are influenced. This is also exemplified in Natifu's (2016) work as an insider. She points out that her insider status was beneficial to her research in many ways, since not only was insider knowledge on institutional culture and setting advantageous, but also "*multiple levels of knowing and being and known*" (p. 219) enabled her to gain access to the participants, to develop good rapport and to conduct open, in-depth and enriching interviews in a more honest environment. Similarly, Teusner (2015, p. 86) underlines that:

> **Over my tenure with the organization, I had developed respect and credibility and was known to be a 'passionate' practitioner. I was well liked at all levels of the organization and was part of the cultural fabric. My insider status was reflected in my years of service and as a member on the operational management team. As I did not work in the factory**

> **environment on a day-to-day basis, my insider status weakened, from a sub-cultural perspective. Nonetheless, the insider status facilitated an understanding of the culture and subcultures of the organization; provided a unique background to contrast perspectives from different participants; and provided sensitivities to the research in relation to political aspects of the corporate environment.**

In the same vein, being an insider at the customer service centre provided me with a position from which I benefitted in many ways. Insider knowledge helped me to identify the institutional culture, structural issues such as the division of labour amongst different departments and internal and external teams and their positions, roles and levels of involvement in the fraud management process. This later proved to be very valuable in identifying different actors in fraud constructions. Furthermore, being an insider was crucial in recognising the diversity of support the company was providing to many national and international retailers, as such information is not shared with the public. This was particularly helpful in understanding the variety of roles employees can take and how this influences their level of experience. Another important aspect was the working requirements and conditions which created constraints for fraud practices. Not only understanding how fraud was managed, but also recognising and analysing this wider context within practices were performed significantly enriched the insights gained from this study.

Furthermore, the identification of possible research participants was also strongly affected by being familiar with team structures and the variety of roles employees could take. It is crucial to understand that organisations can be complex institutions with flexible and not well-defined roles. Given that about two hundred people were based in my department, and employees occasionally had to take on multiple roles and work for different retailers, this simultaneously created flexibilities within fraud-related practices. Being a member of different teams and knowing many employees helped me to develop a profound knowledge of different team structures and their responsibilities and to identify those individuals whose tasks were related to fraud detection, prevention or management. The research will be able to provide a diverse account of fraud practices as a result of the identification of these employees.

Moreover, being an insider was also vital in understanding the technicality of fraud management. Fraud needs to be understood in relation to the technology that generates and classifies data, and related practices that are mediated, influenced and constrained by technological systems. As a former employee, I also worked with different technological tools, which enabled me on the one hand to reflect on the complexities of the technological systems and on the other hand to understand interviewees' points of view and the technical language they used, which may have been too complicated to understand for an outsider.

Despite multiple benefits, being an insider does not mean that access to the research site and participants is guaranteed, as one still needs to negotiate access (Natifu, 2016). As Galletta (2013) points out, some people might act as gatekeepers, which means that it is crucial how the first approach is taken to recruit participants for research. Keeping this in mind, I gave a great deal of thought to what the 'best' method might be to approach my manager. Two points were particularly important for me while planning the first approach. First, I aimed to provide clarity and transparency about my research project while pointing out its significance, and second, I sought to protect the rights of people and the organisation that provided me with this unique opportunity to conduct research.

I decided that these main considerations needed to be communicated clearly in a written format, given that approval requires the knowledge and involvement of different departments and a written document might be easier to pass on. The first step was taken when I wrote down a form of "research proposal" with some background information on the research focus and design and gave it to my manager while briefly talking about my research and addressing these issues. He returned to me on my request some weeks later and agreed that I could conduct my research; however, this would need to go through different departments and would also require their agreement before my proposal could be fully approved.

Costley et al. (2010) outline that organisations can be complex entities in which researchers are not necessarily welcomed or are considered with caution and suspicion. While I was known to my manager, I had no relationship with the decision-makers in other departments. This became particularly apparent when the HR

department contacted me and wanted to view my interview questions, which I provided. In a meeting involving me and the head of the HR department, I clarified once more that my interests were primarily academic and that I aimed to protect the rights of the organisation by providing them with full confidentiality. As a result of information exchange prior to and during the meeting, I was permitted officially to start with the interviews. Overall, it took about 11 months to receive permission from the organisation to interview the participants, as well as to use my own observations and insights for my research.

Bailey (2007, p. 38) underlines that:

> **In some instances, the only person who has a chance of being allowed to conduct research is someone who is already known to the group.**

In my research, being an insider in the organisation provided me with the unique opportunity to access the participants. I am very certain that an outsider would not have been given the chance to enter the site or conduct any interviews, given that the organisation deals with sensitive client data and has legal obligations to protect their rights. As such, they would most certainly not want any sensitive client-related data falling into the "wrong" hands and jeopardising the relationship between them. However, I was given access because I was a trusted member of the same organisation and was well-known to my manager, who in turn had good relationships with other decision-makers.

Another aspect highlighted by Natifu (2016) is how insider status can be helpful in developing a good rapport with research participants and how it creates a more honest and transparent relationship between them. I can relate to this in my own research, as being an insider provided me with a further advantage in the recruitment process and during data collection. As other employees and I shared the same environment, and most people were present during my working hours, I was able to ask my colleagues personally whether they would like to participate in the study. Since most interviews were conducted in the employee lounge in the same building, as preferred by the interviewees, the interviews could be scheduled flexibly during our lunch breaks or after work. Consequently, being at the same location was

particularly beneficial in the recruitment and data collection process. However, sometimes it was a bit loud in the employee lounge. In some cases, other employees wanted to talk but then they had either a brief chat or kept their distance when they noticed that I was conducting an interview.

Moreover, particularly as an insider, I was part of the same company and had many casual conversations with most of my colleagues and a good collegial relationship. This created a more relaxed environment for the researcher and the researched, and it may also have influenced the depth of the interviews. The fact that during the interviews, we were not two strangers, but two colleagues made the interview situation more comfortable for the researcher and the interviewee. Overall, 32 interviews were conducted, with five of these outside the workplace with external managers and the police. Agents[1] were the main participants in this research, as there were more of them involved in daily fraud management practices and the daily decision-making process, as opposed to supervisors[2] and managers, who made major decisions but were limited in number. The vast majority of agents involved in some form of fraud prevention, detection or management practices were part of the research, while very few did not wish to participate or were not available due to holidays and so on.

The participants, particularly the agents, had an international background. Many of them were from other European countries. They decided to move to Germany because of their partners and/or to look for a job. Many of them had a degree. The international background of participants was very welcomed at the customer service centre because they could speak multiple languages, and this was very useful to do fraud examination and contact customers. However, it seemed that many participants were working at the service centre because their level of German made it difficult to find jobs that might have been more suitable to their background.

The criteria for selecting participants were based on the degree of involvement in fraud investigations. The aim was to include participants who were able to provide

[1]Agents as employees deal with specific customer-related tasks such as responding to their emails or calls as well as with fraud-related issues.

[2] Supervisors assign agents to specific tasks and make sure that these are handled on a day-to-day business.

an in-depth account of their experiences in this regard, and so this cohort also included managers, supervisors and team leaders as well as agents. Amongst the agents, there were some people whose main duty was fraud management, while others had other major responsibilities but were nevertheless involved in fraud-related issues to a certain degree. The aim was to include both groups into the research, to build an overall picture of fraud management solely or alongside other responsibilities.

Furthermore, two people working within the police force agreed to participate in this study. While I originally aimed to recruit more participants and conduct more interviews to gain insights into the police perspective, most people whom I contacted informed me that they were not allowed to participate as they are not allowed to give information about their work to an unauthorised person. The reason for aiming to include the experiences of police with fraud resulted from observations in customer services, in that they would regularly contact us regarding specific transactions and ask for information. We would then support the police by providing details so that they could carry on with their investigations. Conducting more interviews with the police could have provided more insights into this unexpected but crucial cooperation. Furthermore, not being able to recruit more people from law enforcement again made the significance of being an insider clear. While I was able to recruit many people within customer services, I was not able to do so while approaching the police as an unknown person, which would certainly have influenced their (un)willingness to share sensitive information with a researcher.

Moreover, Galletta (2013) highlights that participants can be recruited until no new insights can be produced. This was also central to my research. When "a kind of saturation point" (Galletta (2013, p. 33) was reached at the customer service centre, there was no need to recruit more participants. While this was not the case with the police, there was no opportunity to find more participants, and so the recruitment process ended when the number of 32 interviews was reached.

Furthermore, it is important to acknowledge that while being an insider undoubtedly was beneficial in many ways, as discussed above, it can also create challenges, disadvantages and biases (Tanner, 2008; Galletta, 2013). For instance, Costley et al.

(2010) argue that the research can be influenced by organisational structures, settings and existing understandings amongst employees. In addition, the design of the research can be affected by existing relationships and knowledge in the workplace (Floyd and Arthur, 2012), which means that insider researchers are expected to be more subjective in their research design as opposed to other researchers. However, while there can certainly be a close relationship between knowledge acquired in the workplace and the research design, this does not have to be a disadvantage, because insiders may possess profound knowledge of and familiarity with relevant issues and use these to develop new perspectives, particularly when addressing an under-researched area.

Another challenge an insider researcher can face is leaning towards the same position as their colleagues (Costley et al., 2010), because they will be familiar with the same work conditions. Moreover, the researcher might identify themselves with the company and accept existing structures, roles and common practices, thereby deeming them necessary. This certainly was an issue in my research, because while being particularly critical of the normality of fraud management practices, I realised in the early stages of my analysis that I had occasionally similar views to those of my colleagues, since we were simply part of the same environment. This meant that the taken-for-granted work-related practices had also influenced my way of thinking to a certain extent. They had also become partly my 'normality'. Being aware of this issue, I decided that it was necessary to create some distance in order to be more accurate and precise in my analysis. This was achieved on the one hand through the engagement with the literature on social constructionism which helped me to guard against taking fraud management practices for granted, and on the other hand through a new position in the company that made me move away from day-to-day fraud examinations and create the necessary distance.

Furthermore, another challenge can result from a good relationship with research participants, because while insider status enables good rapport with interviewees, it can also create pressures, in that co-workers may agree to participate in the study to do a favour or not to let their colleague down. For instance, Costley et al. (2010, p. 31) underline that:

> **There is the possibility that colleagues may feel obliged to cooperate with your research.**

For this reason, it is important to make sure that the interviewees do not feel pressured to take part in the study, while attempting to maximise the quantity of research participants (Harding, 2013). I aimed to ask my colleagues in a friendly and polite manner for their participation, without giving the impression that they were obliged to support the research project. Some of them responded that they did not wish to participate, which suggests that they felt comfortable communicating their wishes. People who did not agree to participate were mostly people who I did not know very well. I also did not feel that their refusal generated any form of tension between us afterwards given that we carried on sharing the same working environment and occasionally ran into each other.

Moreover, power dynamics can also create challenges for an insider researcher, because, as Costley et al. (2010) note, the researcher needs to be aware of them and their implications when considering junior or senior co-workers as research participants. This aspect is further elaborated in the study by Natifu (2016, p. 230), who underlines that:

> **In my experience the issue of loyalty and not asking too many questions was a real struggle. The power dynamics too further complicated the ease of interviewing these informants, since they were my superiors in the organizational hierarchy.**

Interviewing people who on a professional level were my superiors led to a similar set of experiences where I had to redefine the power relationship during the interview. The interview situation initially created some confusion for me because the manager usually prepared the meeting and made clear the expectations that employees need to meet. However, the interview situation was designed and led by me. While it is often argued that the researcher has more power during the interview, this can be different when interviewing superiors; consequently, it made it necessary to redefine the relationship during the interview and led at least partly to a balance between the roles we took within and outside the interview situation. Initially I felt a

little uncomfortable because he was one the key account managers and played an important role in the company. He was also the first person to be interviewed in a management position. However, perhaps his professional role in the organisational hierarchy created a more relaxed environment for him, thus meaning he gave an in-depth account of his experiences.

A further challenge the insider researcher may encounter is how to utilise their insider knowledge when reflecting on an interviewee's responses (Floyd and Arthur, 2012). This was initially a struggle for me. While I had benefitted from knowing the participants in many ways, being familiar with their work-related performances created in some cases a temptation to fall back into the role of a fellow colleague and to view their responses from this perspective rather than from the standpoint of a researcher. Navigating through this issue required creating some personal distance from the respondents and taking their stories as the starting point of the analysis and not my knowledge about them or their work performance.

Interviewees' responses can also create a challenge for the researcher. During my interviews some participants talked about their fraud detection and management practices and outlined that some decisions were made using racial profiling, disadvantaging certain groups in the society. I found this practice particularly unfair. While I was not able to change it, I intended to raise awareness on this so that this issue is extensively discussed in Chapter Four.

This section discussed how being an insider significantly influenced the design of this research, accessing the site and recruiting the participants. While it was shown how being an insider did indeed result in multiple benefits, the challenges it can create were also explored. This section showed that, as an insider researcher, there is a clear need to be self-reflexive and self-critical throughout the research process. Nevertheless, as Costley et al. (2010, p. 33) observe, insider researchers do not necessarily differ from other researchers:

> **The ethical issues that you anticipate arising in your project reflect your own thinking, which in turn will have been influenced by your situatedness within particular contexts. Like any other researcher, you**

determine which behaviours are observed, which are ignored and how the information is interpreted but, as an insider, you have detailed knowledge of the particular context.

Furthermore, in some cases, even the line between an insider and an outsider researcher can blur. Consequently, it can be unwise to divide them (Tanner, 2008), as an insider may still not enjoy total insider status and *"continually negotiate the continuum of insider-outsider positioning"* (Natifu, 2016, p.232), particularly in complex institutional settings.

Nevertheless, as a researcher, the best efforts were taken to be critical and self-reflexive in designing and conducting this research project while simultaneously respecting and protecting the rights of the participants and the participating company, all of which will be addressed in detail in the following sections. First, though, the following section will discuss the selected qualitative research methods employed in this research project.

3.3 Research Methods

This section will outline the research methods selected for this study. As outlined in the introductory section, this research takes a qualitative approach. As Flick (2014) observes, the research method should be chosen in relation to the research question as well as being guided by the practicalities and contingencies of the research process, including time commitments or financial costs (Galletta, 2013). Furthermore, Boeije (2009) notes that the choice of qualitative research method can be legitimised on the basis that they enable to the maximum the exploration of a new area of study and help create a detailed account of human experience (Marvasti, 2004). Qualitative methods are often not closely defined and are more adaptable to the situation (Hammersley and Traianou, 2012), which can give participants the opportunity to describe their experiences and issues in their own way. Additionally, they can provide the researcher with flexibility in the data collection and analysis processes, particularly when some adjustments are required after the first findings start to emerge (Boeije, 2009). Moreover, qualitative research can also be chosen for

pragmatic reasons, such as the limited quantity of possible research participants (Harding, 2013).

While there is a variety of different qualitative methods, semi-structured interviews are beneficial because, on the one hand, the researcher can prepare questions to explore areas of interest (Berg and Lune, 2012; Lichtman 2013) and, on the other hand, there is room for the participants to go beyond these questions and give insights into unanticipated areas and experiences. They also provide participants with the opportunity to describe their experiences and issues in their own words (Boeije, 2009). Additionally, the interview situation provides an opening for the researcher and participant to probe questions and answers and provide clarification, if necessary (Galletta, 2013).

Furthermore, in-depth interviews imply that the researcher is interested in the experience of other people and gives space and importance to the stories of others. They represent a powerful method of gaining an understanding of social issues based on knowledge developed from the experiences of others (Seidman, 2015). Despite their benefits, interviews can be a labour-intensive process, as they require strong time commitment and include the conceptualisation of the research project, access to and recruitment of participants, interviewing, transcription and analysis (Seidman, 2015).

The choice of semi-structured interviews resulted mainly from the need for qualitative studies, as identified in the literature. Chapter One outlined that there is only limited research available on online fraud and the digital (Kitchin, 2014a; Crawford et al., 2014; Levi, 2012; Pasquale, 2015), so I decided that semi-structured, in-depth interviews would be the most appropriate method to approach this gap in the literature, given that fraud-related experiences could be explored to a greater extent. While interviews can be structured to cover all areas that might appear relevant, interviewees can change the course of an interview, disagree and raise other topics that they might find important.

While qualitative inquiry was necessary to address the research questions and to understand how online fraud is practiced, the practicality and feasibility of the research within the organisation also influenced the choice of research method, given

that there were limited numbers of employees who could be considered as potential participants, due to their experiences with online fraud. The second research method used in this study is autoethnography.

Auto-ethnography is an emerging field of research which is used with increasing frequency in different disciplines to explore social realities from the perspective of the self (Denshire, 2014; McIlveen, 2008; Chang, 2016). This allows the researcher to engage critically with their personal experiences and stories and use them as the primary source of data (Chang et al., 2013; Wall, 2006). Reflecting on personal stories within a particular social and cultural context helps explore aspects of life from a unique perspective. As the researcher studies him- or herself, access to data also remains unproblematic (Kelley, 2014).

Auto-ethnographic research works well when personal stories and experiences as a primary source of data are supported through other sources such as interviews. The combination of multiple sources of data can provide a richer understanding of the research area and strengthen the accuracy as well as validity of information generated through the study of the self (Chang, 2016).

A definition of autoethnography is provided by Natifu (2016, p. 225), who states that:

> **I not only narrate my personal experience (auto) set in an institutional cultural context (ethno), but I also analyse the experienced research process (graphy) looking at the benefits and challenges of the insider research position. I present a personal and self-reflexive account of my research experience in an institution, where I had two levels of cultural experience as student and staff.**

Auto-ethnography is a researcher friendly method and engaging for the reader. Moreover, as there is a familiarity with the data the researcher requires less time for collection and analyses of the data. Additionally, it encourages self-reflection and a critical engagement with oneself within a broader context. However, when taking this approach, the researcher could also be influenced by their own presumptions. They could over-emphasise their experiences and rely too much on their memory (Chang et al., 2016; Chang, 2016).

Within autoethnographic research, the researcher usually takes two roles. In my case, I was a regular employee and a critical researcher who had made many observations on fraud practices over the years. For this reason, it was crucial from my perspective to use this additional source of data for this research. Field-notes were taken, usually after work to write down my experiences, observations and reflections on the workplace practices, on unique cases experienced through the contact with victimised individuals or police or on other relevant issues.

Reflecting on these personal observations and experiences seem to be crucial for two main reasons. First, while the interviews enabled me to gain access to many working experiences on fraud, the interviewees usually used a language which is fairly technical and might often be unclear for somebody not working with the same technological tools. For this reason, being aware of the technicalities of online fraud, and having shared similar experiences, was very helpful in clearly understanding their language and points of view.

Second, the interviews produced data that were related mainly to the fraud management practices of the interviewees. Different accounts of fraud were based not only on their personal views, but also the level of involvement in fraud, for example whether fraud management was their main responsibility or merely a task amongst many others. The interviews, however, provided only limited insights into the role of other departments involved in the process, their working conditions and environment and how these could influence their fraud detection and prevention practices. These issues were not often addressed by the participants, perhaps because they were taken for granted, i.e. they accepted the roles and structures within which they had to operate. However, being a participant and an observer at the same time led to a more reflexive and critical account of personal experiences within the organisational setting and created more enriching data from which this research could benefit.

The exploration of relations between interviewees and their organisation is also a methodological approach suggested by actor-network theory (ANT), since it proposes that there is no ontological division between people and organisations (Roberts, 2012). Furthermore, ANT suggests that we should follow actors and identify the

traces they leave behind. Taking this approach enabled me to follow the employees and track their connections with other human and non-human entities which were crucial in the making of online fraud. ANT does not set a limit for the number of actors that may form a network, which means that the choice needs to be made by the researcher by focusing on the research question.

Moreover, as highlighted earlier, the researcher also needs to be acknowledged as an actor, and so for this reason, they need to be reflexive about their involvement in the research process (Cresswell et al., 2010), which was addressed in the previous section. This section detailed the selected research methods and identified how qualitative research was selected to respond to the research question appropriately and to address the gap identified in the literature. The next section will outline how the interview transcripts were coded and analysed.

3.4 Coding and Analysing the Data

Coding and analysis of the data are a crucial part of doing research. As it is not possible simply to present raw material such as interview transcripts and expect the reader to make sense of it, the researcher needs to make active choices and selections on what to include and how to interpret the data (Boeije, 2009) before presenting them as results. As Silverman (2015) points out, it is incorrect to assume that research findings can "speak for themselves". For this reason, it is also important to provide transparency on how the data were coded and analysed. This process usually starts with coding the data, which refers to grouping similar codes and creating categories; for example, this can include only words, paragraphs or longer texts. Furthermore, when the research involves several participants, it can be helpful to start with data provided by one participant and then code the other participants (Saldana, 2015). While thematic codes can emerge from analysing the data (Given, 2015), the researcher will still make some choices and reductions. However, it is important that this procedure is grounded in the research question (Boeije, 2009).

This research relied mainly on interview transcripts to generate reliable accounts of fraud, while many notes were also taken along the way to keep some of the working

experiences in a written format. At a later stage, personal notes were used to reflect on the interview transcripts, in order to provide clarity, if necessary, or to add more insights. Furthermore, a number of themes and topics emerged from the interview transcripts. However, the coding was guided by the main research question so that while the interviews produced large amounts of data, only relevant information was included to address and respond to the research question.

Upon completing the coding process, the data were scrutinised to reflect on generated themes and categories and then to look for possible biases or a failure to include relevant themes that might have been missed in the first coding phase. As Gibbs (2008) points out, data reliability can be achieved through a rigorous examination of possible errors and mistakes the researcher can make during the transcription process.

Moreover, the reliability of research findings can be achieved through the inclusion of interview quotes (Gibbs, 2008), which would demonstrate that the interview scripts were used as the source of generating research findings. This was done throughout the empirical chapters, as they include a variety of quotes emerging from the interview transcripts. While some interviews were longer than others, and some interviewees provided a more detailed account of fraud than others, the aim was not only to provide the accounts of the interviewees, but also to include a diverse set of quotes to reflect on the diversity of responses. This section explored the coding and analysing process. The next section will examine extensively the ethical challenges and dilemmas that emerged while conducting this research and how these were addressed throughout.

3.5 Ethical Considerations

Every research study will inevitably create a number of ethical questions and challenges, particularly when using qualitative research methods (Silverman, 2013). For this reason, it is important to examine them carefully in advance to ensure that the research is conducted in compliance with ethical requirements that may be defined by the academic institution. As Galletta (2013) outlines, prior to conducting

the study, researchers are required to obtain ethics approval from the university, which usually asks for detailed information on research methods, research design, data collection and storage as well as how anonymity and confidentiality will be assured and how the researcher aims to reduce possible harm that may occur during or after conducting the study.

In this research, approval was granted by three different entities. First, institutional approval by the ethics committee of Goldsmiths, University of London, was given after assessing the submitted ethics form including all the required information on the study as detailed above. Second, approval from the customer service centre was received as detailed in section 3.2, which indicated that I could interview employees outside of working hours and also use my experiences as long as they did not disclose any confidential and identifiable information about customers, retailers and the service centre. Last of all, approval was granted by the research participants through informed consent. All approvals were received prior to conducting the research. My employer gave verbal consent for me to conduct this research, while approval from the university and research participants was given in a written format.

While each of these three approvals was crucial to conducting this study, closer attention herein will be given to informed consent. As Hammersley and Traianou (2012) note, one of the common requirements for conducting social research is that informed consent must be obtained from the participants before the research is conducted. Informed consent refers to the awareness of an interviewee participating in a research project and choosing to do so voluntarily (Berg and Lune, 2012). Therefore, it is important that the informed consent sheet is written in a way that is understandable to the participants (Bailey, 2007) while also making the research purpose clear (Flick, 2014). Nevertheless, informed consent can be a problematic issue in qualitative research. For instance, Marvasti (2004) points out that it is difficult to inform research participants fully in advance about the purpose of the study as well as the direction it may take, given that qualitative research often has an exploratory nature and it can take directions different than originally anticipated at the beginning of the study.

Within this research project, a great deal of effort was taken to inform the research participants transparently about the project as well as their rights. All participants were provided in advance with an information sheet which indicated the purpose of the study, and they were informed that there was no obligation to participate in the research and that this participation must be voluntary. Furthermore, all participants were given a consent form, which they needed to sign before starting the interview. The interview questions, information sheets and consent forms were written in German and English, given that the study was conducted in Germany. Consequently, interviews were also conducted in two languages. The choice of language was given to the participants.

The interviews were digitally recorded with the consent of the participants. Two interviews out of the 32 were not used fully for this research – one was conducted over Skype at the participant's request, but while the interview was being audio-recorded, it become clear afterwards that the equipment failed to record most of the interview properly, so only a very small amount of information could be understood and used. The second interview was disregarded, as we had some personal issues at a later stage. While this situation occurred a couple of months after the interview was conducted and did not affect the insights gained, it made me feel deeply uncomfortable when I started transcribing the interview. After a couple of attempts, I gave up on the transcription, due to the emotional distress it caused me. For this reason, I decided not to use this interview.

Many Interviews were fully transcribed in the original language and were translated into English while writing the findings in the form of quotes, while a few were translated during the transcription process, mainly to present them to the thesis supervisor in the English language.

Furthermore, all audio-recordings and transcripts were – and still remain – securely saved on the home computer to which only I have access through a password. The audio records will be deleted upon completion of this research project.

Another set of ethical questions arise when social scientists enter the lives of human beings. While taking part in the lives and experiences of research participants, they need to ensure that their rights are protected (Berg and Lune, 2012). These are often

expressed through anonymity and confidentiality, which are defined as follows. Bailey (2007) points out that anonymity means that the researcher does not know the identities of the participants, while confidentiality refers to knowing their identities but not disclosing any information about them. Flick (2014) outlines that it can be fairly difficult to provide full anonymity or confidentiality to participants when several people in the same setting, such as a company, are interviewed, because the research participants may be known to each other. Similarly, Costley et al. (2010) note that it also might not be possible to provide full anonymity to an organisation, particularly when it involves an insider researcher, as the organisation is a part of the biography of the researcher.

This was an ethical challenge for this research project as well, because most of the employees were known to me personally and to each other as a result of sharing the same physical environment. For this reason, anonymity could not be provided. However, while the identities of the participants were clear to me, I did not wish to disclose any information about their identities to others and did not wish that their interview quotes would be traced back to them. For this reason, the quotes in the empirical chapters do not include any names at all, with the aim of providing full confidentiality to the participants, not to cause any harm and to protect their rights to privacy.

Another ethical concern was how to provide confidentiality to the company subject to this research. It was clearly communicated from the very outset to my former employer that the name or any other identifiable information about the company would not be disclosed in the thesis or in any other publications. It is also clear to me that my former employer, as a third-service provider, had a great deal of responsibility towards online retailer clients. For this reason, no information about online retailers was disclosed, in order to comply with the interests of the company and not to cause any possible harm. Furthermore, while as a researcher it is important to be aware of ethical challenges and make sure that the research meets ethical requirements in the best possible way, being an employee additionally created the strong moral obligation to remove any identifiable information about the company, clients, research participants and other names of participants mentioned

during the interviews, not only because it was important for me to comply with the ethics of doing qualitative research, but also because they were my colleagues, people with whom I had a good relationships with whom I could identify. This created a stronger sense of responsibility to protect them and avoid any possible harm.

Moreover, protecting the rights of those who cannot speak for themselves was important from my perspective, because the research included very sensitive data about customers' names and identities as well as information on customers who were identified by the police as fraudsters. All identifiable information was removed fully, to eliminate any possible chance of the study being detrimental to the customers or my former employer as the "owner" of the data.

Furthermore, while Hammersley and Traianou (2012) note that the primary obligation of the researcher is to conduct research to address "worthwhile" issues, it is fairly crucial to reflect on ethical issues that will arise before, during or after conducting the research. While participants provide valuable insights into their personal experiences, it should be the responsibility of the researcher to protect their rights and reduce possible risks of harm the research may cause. Additionally, Harding (2013) states that alongside having a moral responsibility toward research participants, researchers are also obliged to conduct ethically informed research for fellow researchers who might use the findings of a current study as the basis of their future studies. As such, ethical requirements, challenges and dilemmas were considered throughout the research and addressed to my best knowledge.

3.6 Conclusion

This chapter provided a detailed account of the methodological and ethical issues raised by conducting a qualitative and insider research study. While it is clear that all researchers are subject to different influences that affect how they design and conduct their enquiries, the aim was to provide as much transparency as possible on the pathways taken to carry out this study. As explored in the chapter, being an insider was very beneficial in many ways, particularly because it enabled access to a critical area of research which would not have been possible otherwise. Furthermore,

insider knowledge was very useful in the identification of possible research participants as well as of other actors who were crucial to fully exploring fraud practices. The insider status also inevitably created some challenges as a result of the role as researcher and employee within the same organisational context.

Moreover, it was detailed how qualitative research methods were chosen on the one hand to address the gap in the literature and on the other hand as a matter of practicality. While the semi-structured interviews enabled in-depth insights into the fraud-related experiences of participants, the additional auto-ethnographic approach strengthened information gained from the interviews and enabled me to be more critical and self-reflexive. The mixed-method approach proved to be very fruitful. Moreover, it was also explored how this research is also methodologically informed by actor-network theory. Furthermore, any research project creates a number of unique ethical challenges and dilemmas, as outlined in the chapter. While ethical concerns were addressed, it was also discussed how the best efforts were taken to comply with the ethical requirements, which not only included receiving approval from the academic institution, the company and the participants, but also meant protecting the rights of the participants and not causing them any possible harm.

The following chapter is the first empirical part of this research and will explore automated and manual fraud detection practices as two interrelated methods that influence how they operate. Furthermore, it will provide in-depth insights into the manual categorisation of genuine and fraudulent customers.

4. The Categorisation of Online Fraud through Digital Data

4.1. Introduction

This first empirical chapter will provide unique insights into manual and automated fraud detection processes and explore how fraud management uses different approaches in conjunction with digitally generated data to construct genuine and fraudulent customer categories. While the aim is to examine the interplay between automated fraud tools and manual reviews, and particularly to explore how genuine and fraudulent user profiles are constructed in the manual process, it is argued that these elements need to be considered as the first key actors in the construction of online fraud. As we move to the next chapters, new actors and processes will be introduced and discussed, thereby generating an overall picture. This chapter will address the first sub-research question of how online customers are categorised through their digital data. The findings explored herein emerged from interviews with fraud agents, supervisors and payment, risk and account managers.

In Chapter Two, it was argued that there is not an "unbiased" way of generating knowledge (Burr, 2015), because each social reality is approached from a particular perspective with specific sets of choices and values and within cultural and historical contexts (Berger and Luckmann, 1966). Similarly, it was observed that scientific knowledge can be considered as a process of production whereby the assemblage and interplay of different actors influences a series of outcomes. In relation to online fraud, it was additionally examined how data played a key part in the construction of profiles of trustworthy or fraudulent users. Data, however, were challenged as a "neutral" ground for fraud examinations, because they entail human choices, selections and biases (Lupton, 2014; Pasquale, 2015) as well as errors and inconsistencies (Kitchin, 2014a). Within this context, this chapter will unravel how fraud as a social reality is approached within fraud management and how realities are constructed based on selected datasets. The chapter particularly examines how fraud results from interplay between automated and manual fraud detection and from the manual categorisation of customers while critically assessing the

assemblage of data as the foundation of building fraud detection techniques and constructing customer profiles.

This chapter is divided into two main sections. The first section focuses on the relationship between automated and manual fraud detection and examines how both approaches are interrelated and how they jointly construct categories of customers. As explored, automated fraud detection tools classify customers – in relation to pre-determined algorithmic rules – as genuine or fraudulent, while customers who do not fit into any of these two categories are forwarded to a manual order review for the final decision.

However, when manual review agents start examining customers' profiles, they can only operate within the given framework of assembled datasets and existing classification and fraud scorings, rather than starting from a "neutral" position. This means that manual reviews are influenced by the prior automated fraud detection process. Manual review agents, though, can overrule algorithmic rules by examining customers and changing fraud scorings through black- and whitelisting, thus demonstrating that the process is a two-way street.

In the second section, a stronger focus is placed on the categorisation of customers through fraud agents within the manual review process while closely examining the data used for generating genuine or fraudulent customer profiles. The section starts by assessing customers based on the consistency of their data and argues that those with inconsistent datasets are more likely to be labelled as fraudulent. This means that when customers enter their details, including their names, email addresses and billing and shipping addresses, any abnormalities in relation to their previous transaction is treated with suspicion.

When there are no previous transactions, customers with matching details, such as when name and email address contain similar information, is given a higher degree of trust than customers with inconsistent order details. Furthermore, it is closely examined which particular datasets are crucial in the construction of customer profiles. The choice of payment method influences whether customers are considered genuine or fraudulent, given that not all payment methods are assigned the same level of risk. Similarly, it is assessed how the housing and area in which

customers live, as well as their ethnic and social backgrounds, affect the level of trust or suspicion they will encounter. The conclusion section provides a brief overview of the research findings and set the scene for the next chapter.

4.2 Automated and Manual Fraud Assessment

This section examines the relationship between the automated and manual review fraud detection approaches. Starting with the automated fraud detection tool, the chart below provides a visualisation of how automated tools sort incoming orders by either accepting or rejecting them or sending them to the manual review team. The data points as shown in the chart represent transactions.

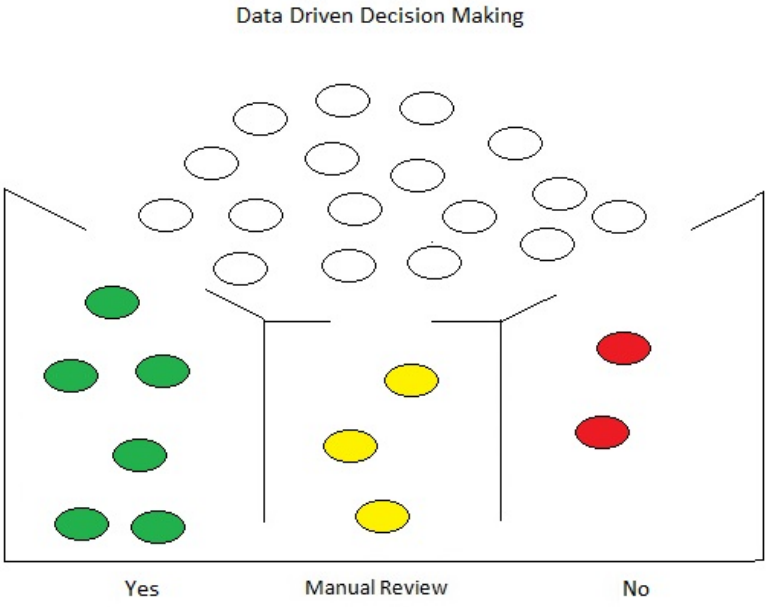

Figure 1. Automated Order Processing

Source: Author's own

As displayed in the chart, orders go through a selection process. Based on a set of pre-determined rules, online transactions are assigned a risk score. This is also because not all orders can be manually reviewed due to limited resources (Polman and Spruit, 2011; Baesens et al., 2015) and the high volume of data. As a result of this process, orders with a high fraud score are declined through automated fraud management tools, orders with no or very little fraud score are accepted, and all the other orders are forwarded to the manual review team for an additional assessment.

As it was argued in Chapter Two, digital activities such as online shopping produces large amounts of data that are collected and analysed (Ruppert et al., 2013; Lyon, 2003). As Gandy (1996) argued, technological tools are used in conjunction with

personally identifiable data to identify and classify individuals into groups of economic value, and to assess whether they are worth targeting. Similarly, Lyon (2005) suggested that with the disappearance of bodies, surveillance practices now target the 'data doubles' of individuals, whereby personally identifiable data are stored and accessed remotely. Individuals are sorted according to different risk categories constructed in relation to technological systems which either provide access or treat individuals with suspicion (Lyon, 2003). As visualised in the chart, the three risk categories 'accept', 'reject' or 'manual review' are defined. When transactions come in, they are classified according to this sorting process. Accepted orders represent inclusion, and denied orders represent exclusion, while a manual review means there is room for negotiation and resistance.

The categorisation of people is made in relation to collected and examined data sets which typically consist of an active and a passive component. The first one refers to data that are actively entered by the customer, such as their names, addresses, email and phone numbers, payment details and the products they select. The second component entails information that is generated in addition to this process. While it can vary quite significantly between fraud detection tools as to how data are collected, the most common methods include device information, user behaviour, the IP and the network (Payton and Claypoole, 2014). Device data can include hardware and software information such as operating system, browser, graphics card and battery level to identify the specific device used for the transaction. This is usually helpful in determining whether a device has been used for multiple and allegedly unrelated orders. The user's behavioural data usually entail information on how the user has navigated through the website, how much time they have spent browsing, whether they have made changes to their accounts and how they behave in terms of how they type. IP and network data contain the IP address of the user and information on their network provider. The generated datasets are then used to create a user profile which is combined to create fraud scorings using algorithmic rules.

While the algorithmic rules can be considered the product of *"unstable associations of people, things, processes, documents and resources*" (Neyland and Möllers, 2016,

p. 2), they gain an object-like status within the fraud management process because they are freed from the conditions within which they were constructed. Furthermore, they become a form of "electronic test" (Bamfield, 2012) and build the foundation for automatically constructing categorisations of good and fraudulent customers while also affecting manual categorisations. This occurs because automated fraud detection tools decide which transactions are reviewed by fraud agents by defining what is suspicious and forwarding only these cases to the manual reviewers. Additionally, as each transaction is assigned a fraud score which implicitly suggests a particular view on the customer, there is a chance that the manual reviewers could come to similar conclusions in their assessments, since they do not enter the process from a "neutral" standpoint, given that an assessment has already been made through the automated system. This is exemplified in the following quote:

> **And when there are many refuses, meaning that orders were cancelled automatically. That's, for example, a negative sign for me personally. The email address and many refuses (Agent, 23 Female).**

As this case shows, a negative assessment emerging from automated fraud detection can result in a similar outcome in the manual review process. While orders can be automatically declined for several reasons, for example for entering payment card details incorrectly, in some cases it can be easier to accept an existing outcome rather than challenging it. One of the reasons for such an assessment can be the overreliance on automated fraud scorings and categorisation, particularly because manual reviewers lack visibility regarding how scorings come together and lead to the rejection of the customer. Consequently, the pre-existing categorisations inevitably influence the action which follows.

This can also be exemplified through a case that I observed. A customer from Belgium attempted to place an order on an international and well-known fashion brand's online platform over a period of time; however, all of his many attempts were unsuccessful. As the person had a key interest using that website specifically, he decided to contact the customer service centre to seek help. The customer service agents, to provide support, looked into his payment attempts, but they soon realised

that all of his order attempts had been rejected by the automated fraud detection. The customer was assigned a fraud score of over 100 points, which meant that the orders were labelled as clear fraud, and so regardless of how many attempts he made, all were stopped in the same manner. Due to the high fraud score, it was not possible for the customer service agents to help the customer move forward with his transaction.

Nevertheless, the customer continued persistently to call the service centre asking for a solution, so the case was escalated directly to the online retailer by my colleague. An examination of the case conducted by the retailer ensued, but it resulted in the same outcome as the automated fraud detection tool, given that the customer's IP was linked to an unusually large number of transactions, which was considered as a sign of fraud. What the online retailer had missed, however, was that the person who they had categorised as 100% fraudulent was one of their own employees and shared the same address as the headquarters of the online retailer. The manager who was based at the very same location had simply accepted the outcome of the automated fraud detection system without seeing the necessity to challenge it. As these two cases show, overreliance on automated fraud detection can influence the outcome of a manual examination as well as make a more thorough examination unnecessary. Surely, in the above example, a more stringent check on the address of the customer would have revealed that he was a regular employee rather than a fraudster.

Moreover, while fraud scorings influence the manual review process, manual reviewers can also challenge the pre-given scorings for future transactions through so-called 'black-' and 'whitelisting'. Blacklisting refers to the process of identifying and blocking fraudulent users from placing online orders in the future, and it can be considered a way of ensuring that the automated fraud detection system recognises a particular customer as fraudulent even though they might not have been categorised as such in the past. This means that future orders will automatically be declined so that it will not be possible for the same person to make a purchase, at least not with the same personal or transactional data. When transactions are

blacklisted, this means simultaneously that the number of manually examined orders will be reduced, because they will automatically be declined as outlined below:

> **At the beginning, we had many more fraud cases in the manual review because we did not have this basis for the fraud cases. The first months we blacklisted thousands of them, if you remember, so the system learned. Now, fewer orders go to manual review, because they are cancelled by the system (Supervisor, 26 Male).**

Whitelisting works in the same way but refers to the opposite process, i.e. when online transactions are automatically declined due to sharing characteristics similar to those previously categorised as fraud. When manual reviewers feel differently about them, they whitelist those customers so that these can successfully place new orders without being stopped by automated fraud detection tools. Furthermore, the availability of black- and whitelisting implies that there cannot be full reliance on the automated rules which determine whether a customer is genuine or fraudulent, because at some point the visibility of automated decisions can be lost, including by those who might have constructed them. Additionally, not all human behaviour can be translated easily into numbers or scorings. Digital systems are a simplification of the world (O'Neil, 2016) whereby human behaviour is reduced to data points. There is a lack of recognition of the context and the complexity of human behaviour (Strong, 2015). Additionally, datasets contain errors and inconsistencies. Patterns can be extracted from non-existent or incorrect data (boyd and Crawford, 2012; Kitchin, 2014a). This makes an additional manual examination necessary.

> **If the system was 100 % right, they would not need any employees. The system will do it (Supervisor, Male 26).**

One of the limitations of automated fraud detection tools is that they cannot relate all personal and transactional data when there are small variations in writing, even if they might belong to the same person. The two following quotes illustrate two scenarios where such recognition and connection of data can be missed:

> **Sometimes, it did not work – the system did not link an address written as 'street' and 'str'., so it would have been easy to see but the system never linked them (Payment Director, 39 Male).**

> **Our system does not match capital and small letters. It is a big problem. It will be normalised. It considers an address written differently as two different customers. This customer used one email but four different credit cards and one PayPal, different names, different IPs, different customer names, different telephone numbers with different ways of writing. Only the email address was consistent every time. If he had used a different email or changed a letter in the email, our system would have automatically seen this as two different customers (Fraud Agent, 26 Female).**

Both examples show some of the limitations of data-driven scoring models. Particularly, they outline how small variations in data can lead to a different outcome. In both cases, the customer can be categorised differently based on a very little change in the way the address is written.

Another limitation of fraud detection tool is that users can bypass blacklisting and place new orders. One way can be by changing some parts of the data as outlined below so that the user is classified as a new customer rather than somebody who has been linked previously to fraud.

> **We do blacklist all the information, but they still place a new order. All they need to do is use a different IP address (Supervisor, Male 26).**

While such a relation in the data can be clear in the manual assessment of transactions, the connection can be missed in the automated process, depending on the algorithmic rules in place. This means that while automated fraud detection tools can respond to large amounts of data and generate real-time categorisations of customers, they cannot completely replace human assessment; as a result, both methods remain as complementary parts of the same process.

The section examined how automated fraud detection and manual order reviews can be considered two interrelated actors in fraud construction. It was explored how fraud detection tools categorise customers as genuine or fraudulent based on their digitally generated datasets, which usually involves creating relations between personal and transactional data entered by the customer alongside other accessible device, user, IP and network information. However, as not all transactions can fit easily into any of these predefined genuine or fraudulent customer categories, selected orders are sent for manual review for additional assessment. This implies that a manual review has been established not only to respond to the grey areas of predefined fraudulent or non-fraudulent behaviour, but also to recognise and overcome the limitations of automated fraud detection. Furthermore, it was also discussed in the section that limitations are prevalent because automated tools are not able to respond fully to the complexity and diversity of customer behaviour. Additionally, while algorithmic rules can relate datasets based on their similarities, data entered with small differences by the same person can be labelled as two different and unrelated transactions.

The findings discussed in this section highlight how fraud construction results from the interplay between automated and fraud approaches and how the data are joined and re-joined in this process. While different sources of data can be merged to generate categories of people, the data can be connected and re-connected in multiple ways also in the manual review process (Van der Schyff et al., 2018; Stoddart, 2014) creating a fluidity and instability of categorisations of customers as genuine or fraudulent.

Further, as previously outlined, while one fraud detection approach categorises certain customers as fraudulent, another one can re-categorise them as genuine – and vice versa. This also exemplifies how thin the line can be between fraudulent and non-fraudulent behaviour. The next section will focus more strongly on the manual order review and explore comprehensively how customers are categorised as genuine or fraudulent, depending on their data.

4.3 Manual Categorisations of Fraud

The previous section discussed automated and manual fraud detection as the two key methods through which customer profiles are constructed. In this second section, a stronger focus is placed on manual reviews. Particularly, it is examined how fraud agents aim to distinguish between genuine and fraudulent customers, using digitally generated datasets. As outlined, the categorisation of customers is achieved based on existing data, how they are entered and how any patterns extracted from the data relate to, or otherwise, the data of other customers.

In Chapter Two, it was argued that businesses use personally identifiable data to sort individuals into social and economic categories. Personal information is used to construct groups based on common characteristics, whereby customer data are no longer only used for identification but to keep records of individuals and maintain or improve businesses (Gandy, 1996, Lyon, 2003). The upcoming sections show that this is not only an automated, but also a manual process whereby customers are examined in relation to selected features and attributes. The examination of their data results in the acceptance or denial of their purchases.

4.3.1 Defining a Suspicious Customer

One of the more important aspects of a manual fraud review is to define what the data can indicate about the genuineness of a customer. One way of approaching this is to check what data the customer has entered, how they entered them and how they differ from what is perceived to be “normal” amongst other customers. Manual reviewers seem to be clear that fraudulent customers can be differentiated from genuine users through their data. Each component of the data entered by the customer is reviewed individually and then related to other information while looking for relations and constructing a genuine and fraudulent customer profile.

Genuine customers are expected to enter matching personal and transactional data; for instance, the name of the customer, the cardholder name and email address are expected to be consistent. While matching data are considered a good sign that the

customer is trustworthy, any inconsistencies cast doubt about the customer, as exemplified in the quote below:

> **For me, first, it's if the data do not match, for example when the customer name, cardholder name and email address do not match. These are negative signs. I release[3] these orders rarely. Only if the customer has called our customer services and said this is me and I am using, I don't know, maybe my father's credit card, my sister's email, my nephew's address, but this is me. Only in this case do we accept this kind of order (Fraud Agent, 26 Female).**

In this example, it is outlined that there needs to be consistency between the names in the order details and the email address. For instance, if the name is John Smith, the email address should also include this name in some form, and the card should also be owned by John Smith. Through data consistency, reliability or trustworthiness is thereby constructed. Furthermore, a clear match between the datasets used in the examined transaction and previous orders placed by the same person is used to create a higher degree of trust.

Additionally, the data are examined in relation to the consistency of the writing of each component and how this could be related to genuine or fraudulent customer profiles. This is exemplified in the following quotes:

> **If an email is written in small letters and everything else in capital letters, then it's definitely a fraudster (Fraud Agent, 26 Female).**

> **That is my opinion, but let's say we have an email address: sometimes they write everything in capital letters and sometimes they write in capitals, small, capital, small. Maybe they think that we are unable to see that it is the same customer (Agent, 22 Female).**

Inconsistencies in writing can also be considered proof that the customer is suspicious or fraudulent. One of the main assumptions is that discrepancies in writing

[3] Releasing an order refers to accepting and processing an order that was previously on hold.

result from copying and pasting users' data found in fraudsters' databases. The second assumption is that fraudsters use this method to bypass fraud detection.

Similarly, a customer's address is also examined to construct categories of customers. Inconsistency in billing and shipping addresses is treated with suspicious, and while many retailers provide the ability to enter different billing and shipping addresses, customers who make use of this option have a higher chance of being labelled as fraudsters. The categorisation of customers based on the addresses is a problematic issue particularly for customer services. As it will be explored in Chapter 6, customers order online and send parcels to their families or friends, go on holiday or move to a different place. This means that they can place orders using two different addresses in such cases. However, some of these orders are then cancelled, due to suspicion of fraud.

Furthermore, customers are also categorised as fraudulent or genuine depending on the frequency of orders placed within a particular time frame and the number of credit cards used for the same or several transactions. This is a particularly relational process, as examined customers are compared with other customers while aiming to define a norm and label those as suspicious or fraudulent who might deviate from that defined standard. This is exemplified in the quotes below:

> **I check if there are any abnormalities, how many credit cards were used (Agent, 55 Female).**

> **When I see that the customer used different credit cards, two or three can still be okay, but if there are four, five or more, then that's very suspicious for me (Team Leader, 33 Male).**

As the quotes show, datasets are examined in relation to the frequency of entered credit card details. One important point emerging from these examples is that based on the data and how often different transactional data have been entered, it should be revealed whether a consumer is genuine or fraudulent. For instance, entering the same credit card details for different transactions over a certain period of time is considered a good sign that the customer is genuine, since, through the continuity of

the same transactional data, the impression is created that the user must own the card. On the contrary, when different transactional data are entered for one or several orders, these customers then have a higher chance of being categorised as fraudulent. Nevertheless, this is a fairly subjective process, and as we shall determine in Chapter Five, manual reviewers vary in their assessment of data and what they define as the norm.

Moreover, the manual categorisation of customers is based on other specific parts of these datasets. A customer's email address and domain are regularly examined to establish what the email address look like and whether it consists of names and numbers, and what email domain has been used. The quote below outlines that the name and number combination is treated with suspicion:

> **These customers who try to make fraudulent purchases invent new things from time to time, for instance the same email with a number in it, and they place an order after another increasing the number: richard1, richard2, richard3 (Senior Agent, 46 Male).**

Additionally, the email domain can also be a decisive factor; for instance, customers entering Outlook and Hotmail email addresses have a higher chance of being labelled as fraudulent than those who use Google's Gmail. Furthermore, customers' details are also examined in relation to the value of the ordered products, whereby customers with high-value orders are labelled as riskier, albeit each retailer might have a different threshold to define this element. However, when customers' details include low-value orders, this can also cast doubt, as outlined in the following quotes:

> **Fraudsters often place many small orders so that it works with Open Invoice (Agent, Male 24).**

> **Well, we had this case as an example where somebody avoided the fraud check by placing many orders for very small amounts. It happened! He took about 2000 euros (Project Coordinator, 46 Male).**

Moreover, customers are categorised in relation to the items they have ordered. While some items are considered riskier than others, customers ordering “high-risk products” are labelled as suspicious. Additionally, the sizing of the items is also considered, in that genuine customers are expected to have the same or similar sizes in their order if they purchase several items. However, if the sizes look random, there is a higher chance that these customers will be categorised as fraudulent.

This section explored how customer profiles are constructed based on what datasets are available to manual reviewers. Particularly, it was discussed that each part of a customer’s data individually examined and then compared to other parts of the same data to create relations. In a further step, the data are assessed in a wider context of all transactions. When a sense of normality amongst the customers is created and the “genuine” customer is defined, any deviations from this norm are treated with suspicion. The specific datasets used for categorising customers are email address, email domain, order value, the frequency of transactions within a particular time frame, the number of credit cards used and product type and sizing. The next section examines payment methods as a key element of the data and which are also used to construct categories of genuine and fraudulent customers.

4.3.2 Fraud and Payment Method

The payment method is an important part of online transactions, because online orders can only be completed after choosing one and then using it to transfer funds to the retailer. As there are usually several payment options available, customers usually choose the option that suits them best, without considering how this might affect their transaction. While the choice of payment option can look trivial when placing an order online, the selected payment method can strongly influence whether a customer is categorised as genuine or fraudulent, because not all payment methods are considered as equally risky. Consequently, the choice of payment method indicated in a customer’s transactional data affects whether they will be considered as trustworthy. Although the payment method alone is insufficient to

accept or cancel a transaction, it contributes significantly to how customers are labelled at the end of the fraud assessment process.

Gandy (1996) argues that identification becomes particularly crucial whenever a cashless purchase is made, for instance using other payment options and as evidence that people are who they claim to be. However, as online purchases are usually made via cashless payment methods, not only is the identification of individuals crucial, but also the risk associated with certain payment methods. In this case, customers are sorted according to their payment method (Lyon, 2003), thereby leading to the generation of sub-risk customer categories. These will be merged at a later stage with other sub-categories to produce a complete customer profile.

The categorisation of customers is generated based on the use of a payment method. While the availability of payment methods varies amongst online retailers and the countries within which they operate, there are some commonly accepted payment options such as debit and credit cards, PayPal, bank transfer and Open Invoice[4], which is particularly popular in Germany. Within the variety of available payment options, customers choosing PayPal as their selected payment method have a higher chance of being labelled as genuine, as exemplified in the quote below:

> **It depends. When I see an order with PayPal, I tend to release the order. Thus, I don't check much but only to see that some data are correct and accept the order. With a credit card, you must be more careful (Fraud Agent, 27 Male).**

As the quote indicates, customers using PayPal as a payment method will enjoy less scrutiny. This is also supported by PayPal's seller protection, which means that in the event of fraud, the retailer will not necessarily have to cover the costs, while this does not apply to credit cards. When manually screening customers' data for fraud examination, those whose selected payment method is Mastercard or Visa might

[4] Open Invoice is a unique payment method, used particularly in Germany, which provides customers with the opportunity to view the product they ordered without making an upfront payment. If customers are happy with the product, they then need to make a payment within 14 days and if not, to return it.

have a higher chance of being related to fraud. However, the risk assigned to credit cards can also vary depending on the financial institution, as outlined below:

> **We know that American Express cards are difficult to get. A customer who wants to get an American Express card will be checked by the bank itself, so we are a bit more relaxed in accepting orders from American Express. Visa and Mastercard are normal credit cards. We pay quite a lot attention to them (Agent, 22 Female).**

Additionally, customers whose transactional data show the additional 3D Secure[5] option offered by financial institutions have a good chance of being labelled as genuine, because an extra security layer is provided. Also, when 3D is in place, online retailers are usually not liable in a case of fraud, as exemplified below:

> **Yes, it is more secure, but also there is a liability shift which is very important, so if we have a transaction that went through with 3D Secure, or we wanted to offer 3D Secure, but the bank did not implement it, we are not liable for any chargeback (Payment Director, 39 Male).**

> **Okay, you can go to 3D Secure and verify after you stole it, but, in this case, we are not responsible. The bank is responsible. The money will come to us in any case. Even if the item gets lost, who cares? The money will be with us. It is a problem for the credit card company and cardholder (Senior Fraud Agent, 46 Male).**

The additional 3D security layer and the liability shift make these online payments safe for fraud management, which means that customers with this option in their payment details will almost always be categorised as genuine. This does not necessarily mean that the customer is genuine but rather that no costs will emerge, even if the case turns out to be fraud thereafter. Therefore, the genuineness of the

[5] This is an additional security layer which requires password authentication. The aim is to reduce the risk of fraud. Companies benefit from 3D Secure payments due to the liability shift, but this could also mean that fraud is not reduced but shifted and displaced to other people or organisations that might not use 3D Secure.

customer is constructed through the liability shift. Additionally, the availability of 3D Secure in the order details can be sufficient to skip a thorough examination. This also applies to prepaid credit cards, as outlined in the quote below:

> **When you see that the credit card is a prepaid credit card, it does not matter if it is stolen or not, because you cannot get a chargeback on a prepaid credit card (Supervisor, 26 Male).**

As the quote indicates, customers with transactional data entailing a prepaid credit card are much less likely to be labelled as fraudulent, mainly because the money is already deposited on the card and cannot be taken back through a chargeback. As these examples show, it is not about whether the transaction is fraudulent but rather who is going to pay for fraud. In Chapter One, it was argued that fraud is a form of deception (Stamler et al. (2014). However, as this example shows, the definition of fraud applied by the employee moves away from a legal or criminological definition and embraces a cost and loss-based perspective.

Furthermore, another commonly used payment method is Open Invoice, which enables customers to make a purchase without making a payment upfront. While this is a popular payment method in Germany, it is used increasingly in other countries as well. Open Invoice is usually considered a risky payment method, because products are sent to customers without the receipt of a payment, as outlined below:

> **Open Invoice is the least secure payment method (Supervisor, 44 Male).**

> **With Open Invoice, you really need to know what you are doing there, because otherwise they are sending some piece of paper and hoping customers will pay. You have to have some good mechanism in place to make sure that you are offering this payment method to someone who is willing to pay (Head of Payment Department, 35 Male).**

As the quotes outline, Open Invoice is not offered to every customer in the checkout process as a payment option, because there is usually a risk score in place to generate creditworthiness. If the risk score is positive, though, Open Invoice as a payment

method is offered, thereby indicating that the customer is trustworthy and will most likely pay for the ordered products. The risk score in relation to Open Invoice works similar to the credit scoring. The objective of credit scoring models is to select the people who will not default (Ball, 2019). However, Open Invoice can also be considered as a small loan given that Open Invoice payments are made after the goods are received. In this case, the scoring models are expected to predict which customers are going to pay for the goods they receive, and which are not so that the customers who are less likely to pay, will not be offered Open Invoice in the first place.

A risk score in the ordering process relies on pre-determined rules to construct categories of customers, as exemplified in the quote below:

> **There are customers who can order for 50 euro using Open Invoice and then we have customers who can order for 500 euro with Open Invoice. It depends on the payment behaviour. Whoever gets a second reminder definitely can't place an order using Open Invoice for the next one-and-a-half to three years (Team Leader, 35 Male).**

> **For example, Amazon in Germany also offer Open Invoice, but their Open Invoice share is 1%. One single per cent. We have the other shop, where we have 95%. Amazon charges consumers for Open Invoice, but consumers trust Amazon completely, so they do not worry so much about paying upfront by card or bank transfer. Large companies can direct people making into such decisions and by adding the fee you are moving them towards making a certain decision (Head of Payment Department, 35 Male).**

While pre-assessment on the creditworthiness of customer influences whether some specific payment methods can be offered, companies can also direct customers *not* to use them, by adding costs. This is an interesting point, because as highlighted above, the choice of payment method will affect how customers are categorised. Being implicitly directed towards a payment method can also mean that the customer

is directed to certain categorisations as the result of their "preferred" payment option.

In addition, while Open Invoice is associated with higher levels of risk, it is considered a safe payment method amongst manual reviewers, which can be understood partly by the fact that fraud management team members have limited access to Open Invoice transactions. They can only see in customers' accounts whether past orders were paid, but they are not able to see whether outstanding payments are a result of fraud or because the customer forgot about it or did not want to pay. Additionally, there is almost no fraud-related feedback received from Open Invoice orders, as these are often handled by external debt collection agencies in the event of an outstanding payment. Online retailers can sell outstanding invoices to a debt collection agency for a percentage of the actual value and then let them handle the matter. Similarly, factoring services can be recruited to externalise the cost of fraud, as outlined below:

> **At that point, I totally don't care whether it is fraud, because my factoring service then has the problem (Account Manager, 38 Male).**

As factoring services handle invoices, fraudulent orders are also handled by and visible to them. Consequently, the internal fraud management team is not confronted with the fraudulent transactions which may affect the perception of risk in relation to Open Invoice and the categorisation of customers who use this payment method. This is another example of how fraud is defined through liability reasoning and probable costs rather than whether the transaction is fraudulent.

Moreover, bank transfer is also offered by online retailers as a payment method. When customers' transactional data include bank transfer as the selected payment method, the chance of labelling these customers as genuine increases, because this payment option requires logging into an account and making a transfer using a Chip and PIN device, which can also be considered an additional security layer. However, whether or not a payment method is particularly secure depends not only on additional security measures, but also on the existing knowledge, as outlined below:

> **I personally don't know the system, but it helps with our work when I see that the customer has always paid with Mercado Pago. Then we can immediately release. How safe it is, I have no idea (Fraud Agent, 35 Male).**

This section closely examined the payment method as a key element in customers' transactional data and discussed how the selection of a specific option can influence whether a customer is categorised as genuine or fraudulent. As explored herein, while customers using PayPal, bank transfer, prepaid credit cards or American Express as their selected payment option are more likely to be labelled as genuine, those preferring Mastercard or Visa are more likely to be labelled as fraudulent. This, however, was not the case when 3D Secure was available, not only because it creates an additional security layer, but also because there is then a liability shift. As the liability shift made clear, the construction of customer profiles results not only from the risks assigned to a certain payment method, but also from the likelihood of costs emerging from a transaction.

Nonetheless, as outlined above, the payment method alone usually is not sufficient to categorise a customer as genuine or fraudulent; rather, it is a key element of the data used to make such categorisations. The payment method is assessed in relation to components of the data discussed in the previous section and in relation to other parts of the data in the following sections. The next section will focus on a customer's address and location and explore how these are used for fraud assessments.

4.3.3 Fraud, Address, Area and Country

This section explores how the address indicated in order details is used to construct profiles of genuine and fraudulent customers. The assessment of an address or postcode is not unique to online fraud and is rather commonly used for the investigation of other forms of risk or fraudulent activity. For instance, Ferretti (2006) points out that the creditworthiness of individuals is usually examined in relation to their address. Similarly, it is used to make judgements about customers within the manual order review process, while looking at variations in addresses and assigning

them a level of risk. For instance, customers entering a rural address as their delivery address are much more likely to be categorised as genuine as opposed to customers who use an address in a big city, since big cities are associated more strongly with fraud, as outlined in the quote below:

> **Some big cities, especially in Germany, France and Great Britain, the more people live in a city, the higher the risk of fraudulent use, because you can just vanish into the crowd, but you can't do that when you live in a rural area, because everybody knows you (Senior Fraud Agent, 46 Male).**

Furthermore, not all areas within the city are assigned the same level of risk. Less privileged areas are considered riskier, and so those living in these areas are more likely to be labelled as fraudulent. The following quote gives an example from Mexico, but customers entering an address in an underprivileged area in Europe are categorised similarly:

> **Really, in many areas of Mexico, where I know no rich people would live, there was an order for 400-500 euros, which I didn't believe. This made this case already suspicious (Fraud Agent, 35 Male).**

Furthermore, the shape and condition of the housing can also be decisive. As shown in the quotes below, there is a higher chance of being categorised as fraudulent if the customer lives in "poor" housing or an apartment block:

> **If it is a big tower block with 150 inhabitants, and you check on Google Maps and see there's lots of rubbish, right in front of the stairs, then it is really hard for me to decide to release it (Senior Fraud Agent, 46 Male).**

> **When I for example see [tower] blocks in France, then that is a bad sign. Most fraudsters live like that, but not always (Agent, 23 Female).**

The better the standard of housing, the higher chances are of being identified as a genuine and reliable customer; for instance, customers living in houses are much

more likely to be labelled positively, not necessarily because the customer owns a house but because the dwelling represents wealth and better living standards so that there is not much doubt whether the person could afford to make a legitimate online payment. Furthermore, for instance, if the house has a garden, a garage or a "nice" car parked next to it, or even in fewer cases a swimming pool, it will increase the value of the customer from the manual review perspective so that he or she will have a very high chance of being labelled as genuine. As it will be discussed extensively in Chapter Five, while customers' data entail the full billing and shipping addresses, external resources are mobilised to assess the condition of the housing or area. This is another example of social sorting (Lyon, 2003) whereby the shape and characteristics of the housing are datafied and used to categorise customers. This case also exemplifies that people from a lower economic background have a higher chance of being categorised as fraudulent which contribute to the already existing disadvantages (Christl and Spiekermann, 2016).

In addition, the country of the customer is also taken into consideration in this research, because manual reviewers undertake fraud assessments for online retailers operating in many European and Latin American countries as well as in Canada, Australia and New Zealand. Each country is usually considered an entity which needs to be examined in relation to other entities. This means that how customers are categorised can go beyond the address they have provided in their details and include the country as an additional dataset. Moreover, not all manual reviewers examine all countries, as exemplified below:

> **I have tried every country. My point of view is, I like Mexico, Argentina and Germany. Some of us only like Europe and some of us like Australia. I think everybody has to know how to do every country. For example, If I'm or my other colleague are not at work, then nobody is doing Argentina and Mexico. They are really afraid of chargebacks – and that is not good (Fraud Agent, 26 Female).**

As outlined in the quote, manual reviewers have specific preferences regarding the countries they examine. While they give specific attention to some countries, others are excluded, which means that the risk constructed in relation to a country or

consumer is not only influenced by the availability of these countries, but also by who works on them. Additionally, online retailers operating in a specific country might have a higher volume of incoming orders than others, thus meaning that more fraud agents will be involved in the assessment of this country, which might in turn affect how the risk is constructed. When a country is assigned a high level of risk, customers resident in that country are also assessed more carefully, as outlined in the quotes below:

> **There are differences, because in France I'm more careful and more precise in any case. It definitely takes five times longer than in Germany (Fraud Agent, 55 Female).**

> **I don't use the same criteria. It is better to accept an order in Australia whenever you are not sure. In Mexico, it is better to cancel the order whenever you are not sure (Supervisor, 26 Male).**

> **I don't like the email address, but it's New Zeeland, it's Australia. I must then tell myself, okay it is only the email address, look at the area and this and that. Then you release it (Agent, 25 Female).**

As the quotes show, in case of doubt, customers are treated differently based on their country of residency. For instance, customers from France can face extra scrutiny based on the risk assigned to this country given that it is categorised as the most risky and problematic country within Europe and requires a thorough examination and can sometimes seem unpredictable, as outlined below:

> **France, I don't like working on France. You know, sometimes everything matches, everything is fine, the amount is not too high, the area is good, the email address, everything is good – and then chargeback… you can't avoid it. That happens sometimes. That's why I don't like France (Fraud Agent, 23 Female).**

As this example shows, working on cases in France represents a particular challenge for the fraud agent, because the customer is categorised as genuine after analysing

the key components of the data (as discussed in the above section) and assessed in relation to other datasets. However, as this case shows, such a categorisation based on the consistency of the data and the level of risk assigned to particular areas, email addresses, order values and so on can change afterwards, because it is socially constructed as to how data are considered representative of genuine or fraudulent customers.

In addition to France, the UK was also initially categorised as a risk country. However, the implementation of 3D Secure for UK payments created a shift in this regard, meaning that customers resident in the country have a higher chance of being classified as genuine, particularly when their order details show the availability of 3D Secure. The quote below outlines how the shift from being a high-risk country to a safe place was made through the 3D security authentication:

> **The UK is quite safe for us, because we can offer 3D Secure, although the UK used to be the most fraudulent market. In 2009, we were implementing all these measurements just to improve the UK (Payment Director, 39 Male).**

Moreover, one of the main countries assessed for fraud examination is Germany, even though it is actually categorised as low risk. The previous section detailed that Open Invoice is a popular payment method in Germany and is assigned a low level of risk by manual reviewers, because fraud resulting from this payment method is handled elsewhere. This means that manual reviewers relate fraud instead to credit card payments, because most fraud-related feedback they receive is linked to credit cards, which are not very prevalent in Germany. However, while German customers are more likely to be labelled as genuine due to their preference for Open Invoice, they can still be labelled otherwise based on the address indicated in their order details, which is then linked to their area of residency, as exemplified in the quotes below:

> **That's of course not nice for the people, but you can't avoid it when you think about it. You can be a very good customer or have lots of money. You move into "an unlucky area", where perhaps the tenant before you**

> **was somebody who never paid his invoices. Then you will be applied the label that you can't be trusted (Supervisor, 44 Male).**

> **Many customers from Berlin get in touch because they can't order, possibly because the address and the area in the city are blocked (Agent, 24 Male).**

Both quotes indicate that an entire area in a city can be categorised as suspicious as a result of previous assessments. When customers attempt to place orders, they will also be labelled as suspicious for entering an address in that particular area. Moreover, in addition to Germany, Nordic countries as well as Eastern European nations are categorised as "safe," meaning that customers resident in these countries are more likely to be perceived as genuine, as outlined in the quote below:

> **Amongst the best is Finland. There, we haven't seen a single fraudster yet. Poland is fairly honest, Czech Republic, Denmark and Sweden, too. Thus, that's not as bad as the rest of Europe. Thus, the North and East are actually fairly honest (Team Leader, 33 Male).**

However, as Eastern Europe represents a new market with low amounts of incoming orders in the manual review process, some changes might occur when the order volume increases. Additionally, Argentina, Australia, Canada and New Zealand are also categorised as less risky as opposed to Mexico, which is considered the riskiest country outside Europe.

In the section above, it was outlined that customer data consist of an active part, which customers actively enter, and a passive part, which is generated in the ordering process. The IP address is captured during the process and collected alongside other datasets for fraud assessment. The IP is used to check in which country the customer is located. An abbreviation of the country and a small flag are then generated to make the assessment easier for manual reviewers. IP can also be utilised to assess whether the customer is actually located at the address indicated in the order; for instance, while an address might belong to Germany, the IP address could indicate that he or

she is in the UK. Customers with inconsistent address and IP combinations are more likely to be categorised as fraudulent, as outlined below:

> **Through the background check, it can be examined whether the IP address is possibly abroad etc., in which case it's already suspicious, because we don't deliver abroad (Backoffice Team Member, 29 Female).**

This is because customers are expected to be at or close to the location of their own delivery address. Perhaps the greater the distance between the address indicated by the customer and the IP, the higher the chances are that the customer will be categorised as fraudulent. While distance can emerge when customers are travelling or using a company IP address showing a different location, many retailers nevertheless treat such a transaction suspiciously. There can however be exceptions not to label customers with an IP address in abroad as fraudulent or suspicious as outlined below:

> **That's also interesting, when we deliver in the UK. For example, we have many Arabic customers who would like to order but are not allowed to do so, because they live, for example, in Dubai. In England, they offer a delivery address in the UK and also a credit card. I don't know how that works, but customers can use credit cards, kind of borrowed, and all parcels are delivered in England and they are then forwarded to our example of Dubai. That's not right. They are theoretically not allowed to do it, but we turn a blind eye (Team Leader, 26 Female).**

This section explored how customers' addresses generated in the order process are used alongside the IP address to construct fraud and non-fraud categories. Particularly, it was discussed that not only is the address used for categorisations, but also the area within the address is located, the country and the geographical location of the country within Europe. Furthermore, it was outlined that customers can also be characterised differently based on the type of housing and accommodation and whether they live in a rural area or a city. The next section explores how the

categorisation of people based on their address also needs to be understood in relation to their social and ethnic background.

4.3.4 Fraud, Social Background and Ethnicity

This section will examine how customer categorisations are constructed in relation to their data entailing information on their social or ethnic background. Automated or manual risk and fraud assessment based on the background check is not unique to online fraud management and can also be found in other areas. For instance, Syal and Haddou (2014) argue that background checks are also used in passport applications, in that ethnic minorities living in identified areas of London are subject to extra scrutiny when applying for a passport, because they have been assigned a higher risk of committing application fraud. Furthermore, backgrounds checks are also usually used for loan applications.

Within the manual review process, the background of individuals is also taken into account when generating fraudulent and non-fraudulent customer profiles. The background of customers is usually assessed through their names, indicated in their order details, while consumers with foreign, unusual or untypical names are more likely to be labelled as fraudulent. There is a similar assessment on the ethnicity of customers, as exemplified in the quote below:

> **There are some places, especially in France, where you can sit the whole day on a bench and will not see a white person. I am not kidding. Even in London it's the same. There are some areas in London you do not have any white faces, only black faces or Chinese faces. […] It depends how often it appears. With some areas and some people, there are no issues. They can be from Morocco, they can be from Egypt, Pakistan or Hong Kong, even from China, not a problem. If there is no issue with the customer, even then I will release it. But there is some doubt in doing so (Senior Fraud Agent, 46 Male).**

This is a good example of how customers are categorised based on their ethnicity. As outlined in the quote, being from an ethnic background can be sufficient to create

doubts about the genuineness of a customer. Furthermore, the quote also shows how whiteness becomes part of the assessment. The following quote provides a similar picture:

> **As I said, I don't want to sound racist, but I cancelled an order in Manchester. I think, somewhere in the UK, because on Google Maps I did not see a single white face. I just cancelled the order. The area looked quite suspicious to me (Supervisor, 26 Male).**

The interviewee indicates in the quote that he does not want to "sound racist," which already implies that there are concerns about labelling a customer as suspicious based on their ethnicity, albeit these concerns are not strong enough to act upon them. This quote also makes clear how being white can positively influence which category the customer will belong to, with non-whiteness leading to a negative categorisation. However, while such assessments are routinely made, they usually remain unspoken.

Interestingly, the same participant highlighted that:

> **Somebody could make a wrong decision because the person is black or from some other country. He is a fraudster because the whole country is shitty. When you are placing a huge order and in your opinion this person can't afford it, according to information on LinkedIn or Facebook, you will cancel it. That is some sort of discrimination, I think (Supervisor, 26 Male).**

This quote underlines that being white is also linked to wealth, or the likelihood of being wealthy. This means that from the fraud management perspective, white customers are more likely to be genuine, because they are more likely to be able to afford the goods, they order than people from other ethnic backgrounds. The agent in the following quote argues similarly:

> **We simply have in France Algerians, Tunisians and so on and so on. These are not fraudsters. That's already racist. I am sorry (Agent, 58 Female).**

This quote reflects how customers are categorised based on their ethnicity, while pointing out that targeting ethnic minorities is a discriminatory process. Benthall and Haynes (2019) argue that discriminatory practices generated through detection models need to be considered within the wider context of how race is socially constructed and how racial profiling exists within the criminal justice system. Discriminatory practices in automated scoring models but also manual detection are a reflection and reproduction of the inequalities in society.

Nevertheless, constructing customer profiles based on name, ethnicity or background is a strong part of fraud management. This can also be observed in the risk assessment process, whereby customers are offered selected payment options as the result of this examination. This is exemplified in the following quote:

> **It will be, for example, although it sounds weird, the name of the customer will be checked. When it is a foreign name, it can be that the order, that the customer, will not have the option to pay via Open Invoice. Of course, it's not *only* the foreign name. For example, it will be checked by the system whether there were fraud cases in the same street (Team Leader, 26 Female).**

As previously highlighted, Open Invoice is a risky payment method. The quote above indicates that only customers who are considered trustworthy are offered this payment option, but the name is also used as an indicator to decide in advance which customers are more likely to pay for the products they order. This also means that customers with unusual or foreign names might have a smaller chance to be offered Open Invoice as a payment method or being categorised as genuine or trustworthy. This section discussed how the names and ethnicity of customers are used to construct categories of suspicious, fraudulent or non-fraudulent customers. The next section will provide a brief overview of the results explored in this chapter and set the scene for the next empirical chapter.

4.4 Conclusion

This chapter aimed to address the first sub-question in this research, namely how online customers are categorised through their digital data. Starting with automated fraud detection, it was observed that relevant tools capture and generate the personal and transactional data of customers, which are then used with the help of algorithmic rules to construct categories. However, given the complexity of consumer behaviour that cannot easily be translated into numbers, selected transactions are sent to manual reviewers for individual assessment. It was argued that on the one hand customer profiles are constructed through the generated datasets and then collated with other data, and on the other hand through the interrelated process of automated and manual fraud detection. The relationship between automated and manual fraud assessment made clear the fluidity and instability of customer categorisations, given that particularly in the manual process, customers can be re-categorised, thus creating a shift between being a genuine and a fraudulent customer, or vice versa. This process revealed how thin the line between fraud and non-fraud can be and how easily such categorisations can change.

The construction of customer profiles was explored in detail within the manual review process. Particularly, it was examined how customers were characterised based on the available datasets and the way the data were entered while creating relations between each component of the data and looking for matches or inconsistencies. While customers entering consistent personal and transactional details were considered genuine, those with unusual combinations or inconsistent datasets were more likely to be suspected of fraud. Furthermore, it was discussed that particular datasets were given more relevance, such as the address, email address and domain, order value, product type, product size, the frequency of orders within a certain time and the number of credit cards used for transactions.

The payment method was also explored as a key component of data, given that customers were categorised depending on their choice of payment method, while some payment methods were considered safer than others. Particularly, it was observed that customers using PayPal, bank transfer, prepaid credit cards and American Express were more likely to be considered genuine, while individuals using

other credit cards were more likely to be labelled as fraudulent. It was also shown that the liability shift played a crucial role in classifying customers, because the definition of being genuine was extended to those transactions whereby, in the event of fraud, the retailer did not have to pay for the costs.

Similarly, it was explored how the address entered in the order details was used for profiling customers. This assessment of the address was extended to the area, the city, the country and the geographical location of the country within Europe. While customers living in "good" housing, rural or wealthier areas or particular countries were more likely to be categorised as genuine, customers living in big apartment blocks, less-privileged areas, big cities and other countries were more likely to be labelled as fraudulent. Additionally, it was examined how the names and ethnicity of consumers were also used to construct categories of genuine or fraudulent customers. As discussed, customers with foreign or untypical names were more likely to be viewed as fraudulent. However, it was also argued that the construction of customer profiles does not emerge from assessing a particular dataset but rather in combination with the assessments made on other datasets of customers. This means that there are multiple ways in which fraud or non-fraud categorises can be constructed and re-constructed.

In Chapter Two, it was discussed that data-driven practices are problematic in several ways. As argued, data cannot be considered neutral representations of people, because they are the result of human choices and selections (Lupton, 2014; Pasquale, 2015). Additionally, data can contain errors and inconsistencies, which are then joined with other datasets to construct categorisations of people through algorithmic rules or a manual process. Furthermore, data are often repurposed and used in ways which were not the intended usage when originally generated (Kitchin, 2014a).

This shows that on the one hand selected and imperfect datasets are used in conjunction with algorithmic rules, and manually, to construct realities about customers while generating a complex process whereby the steps in these assessments are no longer traceable. On the other hand, customers are not able to challenge the outcome of these assessments, because such practices are kept secret; as such, the outcome is taken for granted and freed from the conditions within which

they were created. As a result, some customers then become genuine and others are fraudsters, but it also creates categories of inclusion and exclusion (Crawford, 2013).

Furthermore, it was argued in Chapter Two that social constructionism explores social realities through the role of human actors. This empirical chapter, however, showed that online fraud is constructed in relation to data and technology. It was also discussed extensively how multiple constructions were possible, based on how data were assessed, joined and re-joined with automated or manual approaches. The findings explored in this chapter can perhaps be considered the first step or one way of understanding how online fraud is constructed. As we move to the ensuing chapters, other relations and processes will be revealed. The next chapter will build on these findings by exploring how social practices are performed, by utilising internal and external datasets and mobilising additional resources.

5. Fraud Construction Practices

5.1 Introduction

The previous chapter discussed extensively how the profiles of genuine or fraudulent customers were constructed in relation to the assemblage of data and the interplay between automated and manual fraud detection. This chapter will explore how online fraud is constructed through social practices. This is the second sub-question of this research. The aim is to expand understanding developed in the previous chapter by empirically examining how fraud results additionally on the one hand from how humans utilise data for fraud assessments and on the other hand how individual and collective practices influence what constitutes online fraud. In Chapter Two, it was argued that the development, transmission and maintenance of all human knowledge are constructed in social situations (Berger and Luckmann, 1966). This chapter will examine how manual reviewers develop, maintain and negotiate social practices with the aim of distinguishing between genuine and fraudulent customers.

The chapter is divided into two main sections. The first section will examine how manual reviewers utilise data to make individual or collective fraud assessments. Starting with data-driven practices, it will be investigated how manual reviewers assess the personal and transactional data of customers based on the cases they have viewed and examined before. This means that they place the current transaction within a historical context and make decisions based on how such cases were examined and decided in the past. While this is a predominantly data-driven routine, manual reviewers also develop subjective practices that go beyond an examination based on data. Subjective methods refer to the individual examination of transactions while relying on feeling, experiences and intuition. This practice shows that fraud is often not determinable but is constructed through a fairly subjective process.

Collective practices are performed similarly and include at least two members of the fraud team who examine cases and propose and negotiate ideas on how to categorise customers. A collective examination of fraud is usually initiated by a manual reviewer who seeks support from team members in the assessment of a specific case they might perceive as challenging or difficult to decide on. Fraud agents then discuss

together the transactions using their ideas, understandings and preferences. A decision is made based on which arguments are brought up and whose arguments are given more weight. Another practice developed by the manual reviewers is called the experimental cancellation, which is performed when manual reviewers cannot decide clearly whether or not to accept a transaction despite individual or collective fraud examinations. Through the cancellation, they aim to test the legitimacy of customers or to provoke action. If the customer returns to customer services regarding the cancellation and is able to "legitimise" themselves, manual reviewers re-categorise the customer and enable them to place orders in the future.

The second part of the chapter will explore external practices performed by the manual reviewer, namely the process of moving outside the datasets generated in the ordering process and mobilising other actors to support fraud decisions. As will be discussed in the section, there are two main external practices. The first one is the so-called web verification, which refers to searching a customer's specific datasets on the internet to find relations. In this case, specific websites and internet platforms are considered as actors who can confirm if the customers are who they say they are. The second practice is phone validation, which refers to contacting customers via phone and confronting them with a number of questions with the aim of finding out whether they are genuine, based on their responses and the way they provide these responses. In this case, the customer is the main actor in validating their own identities, albeit without being aware of the process. The final section will provide a brief overview of the findings explored in this chapter and set the scene for Chapter Six.

All social practices explored in this chapter are parts of the same process while in some cases manual reviewers might focus on a single practice to make a decision, and in other cases they may choose to combine different methods before accepting or declining a transaction. This means that multiple constructions of fraud are possible based on which practices are performed and how these are related and extended to others. Furthermore, fraud is constructed based on assembled and accessed datasets, existing and varying understandings, personal preferences, group dynamics and how all of these relate to each other. Social practices are developed

and maintained by the manual reviewers, because uncertainties remain despite the data and data-driven categorisations explored in Chapter Four. While these can provide manual reviewers with some support, fraud decisions still remain challenging, because they are the product of a subjective process rather than knowing the identity of the fraudster.

5.2 Internal Practices

This section will examine how manual reviewers develop a number of internal practices using data generated in the ordering process. Before moving to the exploration of these practices, it is perhaps useful to underline once more why they are essential for manual reviewers. As pointed out earlier, fraud management is a very challenging process, because customers' real identities are not known to the manual reviewers, so they attempt to find out through various means if the customers are really who they say they are. As this is a proactive process, there is only limited "evidence" to show if the customer is genuine or fraudulent. Only when fraud has been successfully committed and notified can fraud agents know that the transaction was fraudulent, which is then usually too late. Consequently, the proactive assessment creates a major challenge for manual reviewers, as exemplified in the following quotes:

> **We are not fortune tellers (Agent, 26 Female).**
>
> **People are different, and you cannot of course look into their minds, see what they think (Agent, 23 Female).**
>
> **Sometimes, there are orders and I have no idea what to do (Agent, 25 Female).**

These quotes outline the complexity of predicting fraud particularly, because many transactions either look alike, without any outstanding datasets which could be used to link them to pre-defined categories of fraud, or they are so unique or diverse so that they also do not fit into identified groups of genuine or fraudulent customers.

Consequently, manual reviewers develop particular routines to make fraud decisions. These are explored in the following sections.

5.2.1 Data-Driven Practices

This section will examine how manual reviewers utilise the personal and transactional data of customers for comparison purposes, in order to construct categories of genuine and fraudulent customers. This entails examining online transactions in relation to previously examined cases while looking for similarities between them. The categorisation of transactions as fraud or non-fraud is then highly influenced on the one hand by whether similar cases were observed and on the other by how they were labelled. This means that online fraud is assessed within a historical context whereby understandings of past cases are transmitted for examining the transactions at hand. This is grounded on the pre-assessments of the data, as addressed in the previous chapter, through which genuine or fraudulent transactions are defined.

Fraud assessments can be less challenging if the transaction of a specific customer relates to their past transactions or those of other customers. Particularly, the customer is placed within the context of their order history while their datasets are compared with those for past orders. The stability of these datasets is used to generate customer categories. This is, however, a rather complex process, because in many cases such expected stability is not given or can change over time, as exemplified in the quote below:

> **Sometimes, I am positive because it is an existing customer. He has used one credit card, one email address, he ordered in 2013 and had seven orders and then four were chargeback and then he disappeared. I was like, okay, but everybody else would have accepted him. Everything seemed to be normal, nice, like an existing customer [Customer with an order history]. Everything matches and four chargebacks. You never know (Agent, 26 Female).**

This quote displays the instabilities in data caused by chargebacks. As previously outlined, a chargeback refers to the return of funds to customers, due to an

unauthorised payment or a dispute. Chargeback is often considered an indication of fraud, which means that the payment details were used by somebody else other than the cardholder. In the above example, the customer is re-categorised as fraudulent following the receipt of a chargeback. This case also underlines that the generated or collected datasets are not necessarily static and can change over time, alongside customer categorisations. The change in data, however, creates uncertainties for manual reviewers because of the contradiction between the customer categorisations in relation to their past and present transactions. This case also makes clear how fluid the concept of online fraud is and how it can change alongside data generated in the ordering process and thereafter.

The following quote also exemplifies the limitations of examining fraud within a historical context, given that the uniqueness and diversity of customer behaviour can be reflected through their datasets and these do not necessarily fit into existing understandings or pre-defined customer categorisation.

> **Every day is not the same challenge. We think we have seen everything, but every day something new pops out, something really incredible or confusing (Agent, 26 Female).**

The following quote also exemplifies how challenging the assessment can be when there are no historical data:

> **It became difficult when all the details were placed for the first time. It is an absolutely new customer. We don't know the name, email address, IP address, the credit card; never seen any of it (Agent, 21 Male).**

As outlined in the quote, first orders cannot be considered within a contextual framework, due to the non-existence of previous data that could otherwise be used to make comparisons.

Data-driven practices are developed by manual reviewers as a means to define manually genuine or fraudulent customers through the construction of relations between past and present transactions. However, there are strong limitations to this

method because of the uniqueness and diversity of the data, which cannot be assigned to any of the pre-determined categories of fraud or non-fraud. Furthermore, a lack of data particularly for single transactions, as well as the changing character of historical data, contributes to the limitations of this approach. As a result, additional procedures are developed by manual reviewers to make fraud assessments. The next section will examine how fraud is constructed through the subjective assessment of online orders.

5.2.2 Subjective Practices

As explored in the previous section, when manual reviewers make data-driven examinations, they encounter challenges due to limitations of the data as well as to taking a historical approach to fraud. This section will explore subjective fraud assessments as an additional practice developed alongside data-led examination, which refers to fraud evaluation based on personal feelings, judgement and experiences. While manual reviewers also perform subjective assessments on transactions to overcome the limitations of pre-defined categories of genuine and fraudulent customers, the following quotes show how both approaches could create a contradiction between customer categories:

> **My point of view is, I can't find anything, but I have a really bad feeling, so I cancel it. Sometimes, you can't explain why you feel this way, but in most of the cases it is correct. It is like a sixth sense (Senior Agent, 46 Male).**

> **There are customers where everything looks good. But because you basically never get directly in touch with the customer, you can of course only decide based the information you have, and with one you decide it is right, then it's right. With another you have the same indicators and using your experience you decide that he will not commit fraud – and then he commits fraud anyway. Well, it is always difficult to weigh up (Team Leader, 33 Male).**

Both cases exemplify how customer profiles are constructed based on individual judgements and feelings, or via a "sixth sense," rather than on data and how personal assessments can result in fraud decisions even if there are no supporting data. Additionally, while data-driven fraud examination usually focuses on how data are assembled to categorise customers, the second quote also outlines that this does not necessarily work, as two transactions with same data structures can lead to two different outcomes.

Similarly, the following quotes exemplify how manual reviewers use their experiences to overcome the uncertainties of identifying genuine or fraudulent customers:

> **It is always a shot in the dark, I would say. You can just hope that your feeling is right. But what I saw in the beginning was that it was really bad, received too many chargebacks because I was not looking at the right things. With the time and experience you get this kind of feeling that you are taking the right decision (Agent, 22 Female).**

> **I must say, I started in October but in December and January I felt sure about what I was doing (Supervisor, 26 Male).**

As both quotes outline, manual reviewers feel more secure about their decisions after some experience with fraud. Nevertheless, the experience does not provide agents with 100% certainty that they are making the right decisions; rather, it gives them more reassurance.

Another subjective approach utilised amongst manual reviewers is to weigh up arguments that speak for and against the customer, using the data, their judgements and experiences. While this is an individual process, the next section will show this can also be a group practice. In this case, the categorisation of the customer as genuine or fraudulent results from the outcome of an individual assessment, particularly from how many pro or contra arguments were generated in this process and which were given more weight than others. However, customer categorisation can still remain challenging, as outlined in the following quote:

> **It is always different. With some orders, it's 50-50. I take a risk because you can't call all customers. I just release it. I don't know 100 % that it is not a fraudster, but if there are not many doubts then I just accept it (Agent, 27 Male).**

This quote implies that the uncertainty remains despite the individual fraud assessment which goes beyond the data in order to provide manual reviewers with additional support. However, because fraud agents do not have the possibility of knowing in advance which customer is fraudulent, in some cases they take the risk and hope that they have made the right choice. Subjective practices are a good example of how constructing the profiles of genuine or fraudulent customers results from a very individual process aligned with varying personal judgements, preferences and understandings. The next section will show how this can also be a collective process.

5.2.3 Collective Practices

The previous two sections discussed two individual approaches along with their limitations. This section will shift the focus to collective practices performed by manual reviewers, particularly to overcome the limitations of individual fraud assessments. It was previously argued, constructionist perspectives suggest that everyday knowledge is constructed through the use of language (Burr, 2015; Gergen, 2015). Language is considered as a medium through which shared understandings are created and realities are proposed (Burr, 2015). Social interaction also plays a crucial role in the collective assessment of fraud.

The collective evaluation of fraud entails an assessment process involving two or more members of the manual order review team, whereby different fraud understandings, ideas, judgements and realities are proposed and communicated, and some arguments are given more weight than others. Fraud then results from the outcome of the negotiations between the team members. This practice is performed particularly when manual reviewers examine challenging and conflicting cases, as illustrated below:

> **I make some decisions by myself and some also in the team. In the team in particular, as I said, when the amount is too high and when I also have doubts due to the area (Agent, Female 23).**

> **With some orders, what we do first is to ask others. We work a lot as a team in this sense, I don't know, if I am being too suspicious towards the order or the person. Can you look at it for me (Agent, Female 22)?**

> **You can also definitely talk about it together, just to also hear other information and opinions. Others search online completely differently than yourself. Then it is better than pursing a trace that doesn't get you anywhere (Agent, 55 Female).**

These quotes reflect individual reasons for performing a collective fraud assessment. As outlined, manual reviewers consult their team to compare between their own assessment and the assessment of others, in order to address their doubts. This is because some cases are considered particularly unique, in which case the group discussion helps fraud agents to review, challenge or confirm their individual assessments. What counts as fraud is then influenced, for example, by whether the case is discussed in the group, how many agents are involved in the discussion, what data are used for the assessments, whose arguments are stronger and given more weight, how experienced the agents are and how they understand risk.

The following quote shows how fraud construction results from the combination of various individual and collective practices:

> **Well, I look for arguments which stand for or against the case and then present them and listen to counterarguments. We weigh up how it can be. We check it again on the internet or the data the customer provided us with and decide based on the discussion which is the more likely version (Team Leader, Male 33).**

This quote underlines that many approaches are taken within the same process and for examining the same case. The aim, however, is not be 100% certain in the identification of genuine or fraudulent customers, as manual reviewers are aware of

the limitations of these proactive fraud assessments, but rather to make as accurate a decision as possible. Collective fraud examinations can also be challenging, though, because many reviewers vary in their understanding and assessments of fraud:

> **I prefer to cancel the suspicious order, but another colleague prefers to call them. She is not ready to cancel it. Our client returned to us on a chargeback case. She asks me what I think, and I say cancel it, but she is like no, maybe he is not a fraudster and I give him a chance. No, cancel it. Sometimes, I can cancel too many. Like a normal customer tries 20 times and I cancel, cancel and cancel and she asks me why did you do it? For me, it was not okay (Agent, Female 26).**

This is a good example of how two different fraud understandings can clash in the examination of the same case. As the quote shows, while one agent aims to accept the transaction, the other prefers to cancel it. These two different views are then negotiated, with one of them representing the final outcome based on the arguments both agents bring to the discussion and which is given more weight. Furthermore, it is outlined in the following example how varying understandings of team members influence the assessments of their co-workers:

> **I would ask A., who would say cancel it. Had I asked M., then he would have said release it. Well, you can see, everyone has other experiences and they can point you towards something which you did not think about (Agent, 25 Female).**

As outlined in the quote, the outcome of the collective fraud assessment can vary based on which co-worker is consulted. Furthermore, the quote also shows that the willingness to accept others' fraud understandings over one's own views can depend on the degree of experience the other person might have.

Another collective method performed by manual reviewers is the examination of chargeback-related transactions. As previously discussed, chargeback claims are usually made when a transaction was not authorised by the cardholder. This means that these transactions were initially labelled as genuine but are then re-categorised

due to the receipt of a chargeback. Such cases are usually examined individually and discussed in the team with the aim of developing a common understanding, as outlined below:

> **I think we see a chargeback from Visa, MasterCard and American Express once a week or so, or every two weeks. What we do now is that one of us works on the chargebacks and blocks the customer's email address, credit card and so on. We have an Excel table, so we can see who did what. We write the names, so I can pay more attention to, for instance, this country combination or maybe I need to pay attention to customers who place an order twice a day with little time between the two (Fraud Agent, 22 Female).**

As the quote underlines, chargebacks can be used to review individual and collective fraud assessments, as they serve as proof that some previous assessments were incorrect. Similarly, the lack of any chargeback can be understood as a confirmation that the fraud assessments made automatically or by manual reviewers were correct. However, as addressed in Chapter One, using a chargeback as an indication of fraud is problematic, because not all fraud cases come back as chargebacks or all chargeback claims result from fraud. As it was outlined, customers can also make a chargeback claim when they ask for a refund for other reasons.

Furthermore, a common understanding in the team is also developed through making each fraud decision transparent to others by writing comments on customers' accounts after the examination of each order. The comments usually contain a reference to the relevant data, including a long order history of the customer, consistency of the data such as matching customer and cardholder names, email addresses or any inconsistencies through varying order details such as different names, addresses and credit cards and so on. The comments are written so that co-workers can see why their colleagues accepted or declined certain transactions:

> **If we don't write down this whole bunch of information, the next person will accept it. That isn't acceptable. The next person who opens this case should know every small detail. For some cases I write a long**

> **explanation why the orders should not be accepted, I spent like 15 minutes on that and the next person who has never done Mexico, oh two positive orders I accept that, even with another email, credit card and other details (Agent, 26 Female).**

As the quote underlines, the aim is also to pass on one's own understandings to others, to encourage them think along similar lines and make similar decisions. However, as this example shows, such information can also be missed by other team members, particularly due to limited time available for fraud examinations. As will be discussed in Chapter Six, quick decisions are required to deal with large quantities of data which contribute to whether other colleagues' assessments are taken into account.

This section discussed how manual reviewers make fraud decisions by including other team members in the process, and how fraud results from the collective evaluation. Furthermore, it was explored how certain practices are performed in the team, to develop a common understanding of fraud. The next section will discuss the final internal method of experimenting with order cancellations as a way of confirming the genuineness of customers.

5.2.4 Experimental Cancellation Practices

This last approach refers to order cancellations with the intention of testing customers' reactions, provoking a reaction or validating legitimacy. The agents consider this process an experiment, as through cancellation they aim to explore whether customers will challenge them. Through the way the customer reacts, the fraud agents review their initial assessments and can take different actions for future orders. As Lyon (2003) argued, how risk categories are constructed and operated is partly affected by the acceptance, negotiation or resistance of those subject to data-driven surveillance practices. In this case, resistance is welcomed by fraud agents seeking to review the initial assessment of the customer and to overcome their own uncertainty in terms of making a fraud decision.

Cancelled orders, however, are not necessarily considered as fraudulent – they might simply be too unusual or too risky to accept. Cancellations might seem to be a safer option than releasing the order, as exemplified below:

> **If it doesn't personally convince me, then I'm sorry. Then we rather wait for a ticket, which means the customer gets in touch. When the customer doesn't get in touch, then I was probably right (Agent, 25 Female).**

As the quote outlines, customers who are "genuine" are expected to challenge this practice by getting in touch with customer services and raising their voices. This can then be considered as proof that the previous assessment was incorrect, and the next decisions should be made in favour of the customer. However, if the customer does not get in touch, then manual reviewers can conclude that order cancellation was the right thing to do. As the next quote shows, customers usually react to the cancellation with dissatisfaction:

> **There are some who feel they have been treated unfairly because the order was cancelled. But mostly these are also customers where you can't really say whether it is fraud or not (Team Leader, 33 Male).**

The quote implies that while customers can challenge this practice, order cancellation can still cast doubts about them. Nevertheless, the responsibility is implicitly shifted towards the customer, who then needs to prove that they are genuine by contacting the service centre. However, even if they do get in touch, this does not necessarily mean that they are genuine, and if they do not contact customer services for whatever reason, there is a high chance that their future orders will be blocked. This is also illustrated in the following quote whereby previous order cancellations by some team members influence how other team members approach the same customer:

> **It is a bit different when the customer has already previously ordered, and the order was cancelled by one colleague. Now the customer orders again, and in my opinion the customer is not a fraudster and it is a**

> **normal order which I would personally release. But I don't do it for now, because maybe the colleague found a reason for the cancellation. Then I think about whether to call the customer and get everything confirmed (Fraud Agent, 27 Male).**

As this quote shows, manual reviewers consider their fraud examinations in relation to those of other team members and are affected by how previous orders were decided upon. This case is another example of how fraud assessments result from a subjective process. This section explored how fraud is constructed through individual and collective practices based on internal datasets, individual preferences, group dynamics and existing understandings thereof. However, as discussed, fraud decisions still remain a challenging undertaking, and so, for this reason, manual reviewers also develop other methods by mobilising additional actors, which will be explored in the next section.

5.3 External Practices

The previous section discussed how manual reviewers develop a number of practices using internal datasets to construct profiles of genuine or fraudulent customers. However, as internal datasets provide very little support for manual reviewers making fraud decisions, they also develop additional procedures. In this section, two main external methods will be explored. The first is Web verification, which refers to searching for customers' details on the internet to find a relationship between the datasets generated in the order process and those accessed on the internet. Web verification, however, is not unique to online fraud prevention and detection. As Tracy (2005) points out, background checks via the Web can be performed for various purposes, particularly for identity checking or to examine the physical existence of the address.

Examinations of customers' identities and their personal and transactional data are also performed through so-called phone validation. Manual reviewers aim to find out through phone validation whether the number provided in the order details is correct and assigned to the person placing the order, and whether the customer is able to

answer questions posed by fraud agents (Montague, 2010). One of the main differences between both approaches is that during Web verification, Google and social media platforms are the main validators of the information provided by the customer, while phone validation requires customers to authenticate their own identities. Both serve as an additional verification measure to scrutinise whether the customer is who they claim to be and whether they are reliable or trustworthy. Through these additional routines, manual reviewers categorise customers as genuine or fraudulent.

5.3.1 Web Verification

This section will discuss how manual reviewers search for customers' details on the internet and use these to differentiate between genuine or fraudulent transactions. Web verification is a powerful tool used by manual reviewers, particularly when mobilising platforms like Google Search and Google Maps as well as social media websites as actors. While Google Search provides access to many websites and platforms, where customers' order details can be compared to their original data, Google Maps provides images of the housing and location of customers. As Dupont (2008) points out, Google Earth provides good quality images which can be used to examine the housing or the neighbourhood of a customer and then to categorise them as genuine or fraudulent. Fraud then results from the outcome of how this practice is performed and which other actors are mobilised, what data are accessed and how these relate to personal perspectives and understandings of fraud.

The following quotes illustrate how often Google is utilised by manual reviewers for fraud assessments and as a support for individual or collective decision-making:

> **I use Google every time, and of course it helps me with my work (Agent, 23 Female).**

> **I use Google very much (Agent, 35 Male).**

> **Google? Almost with every order. Very often (Agent, 27 Male).**

Probably every time, when I work on an order (Agent, 25 Female).

Rather every 10th or 15th [order], I try to avoid it, just to come to a quick decision (Team Leader, 33 Male).

As the quotes indicate, Google Search and Maps are used by all members of the team, albeit with varying frequency. As discussed previously, not being able to know factually whether a transaction is fraudulent creates a major challenge for manual reviewers. Google is used to overcome this challenge in the hope of finding an external actor who can validate and confirm that the customer has indeed provided their own data and they are indeed who they say they are. This is a particularly important point because of the uncertainties created in the digital environment whereby fraudsters easily impersonate others.

From the fraud management perspective, a customer verified through the websites and platforms accessed in Google is a good and reliable customer. These customers are then classified as trustworthy and considered genuine, which not only affects their current transactions, but also other online orders in the future. The following quote shows that this practice is used to verify the data provided in the order details:

You have the possibility to verify them, and then it is even easier for us (Senior Agent, 46 Male).

In this case, Google also becomes a means of comparison between the personal and transactional data of customers on online retailers' databases and additional sources accessed through Google. The verification is performed by searching customer's details on Google, such as names in relation to the city, while looking for consistencies or inconsistencies between the datasets generated through the ordering process and other websites accessed through Google.

I try to verify the customer via the Web, which means looking up the name, surname and the city (Agent, 22 Female).

First, I look for the name and if I can relate it to the place (Agent, 55 Female).

As shown above, this is a relational process whereby some parts of the data are looked up in relation to other parts while searching for matches. Customers are then categorised as genuine or fraudulent based also on whether Google can "confirm" that the person is who they claim to be, for example when Google search results also indicate that the customer is resident in the city shown in the order details. Another key part of the data used for Google Search is the email address. Customer email addresses as provided in the order details are usually Googled to search for similarities. Customers are considered genuine when Google Search results lead to specific websites where there are the same data, or combinations of the same datasets can be related back to the customer.

Similarly, manual reviewers also look up customers' phone numbers to verify them through digitally available phone books or other sources. When the customer's phone number is listed, for example in a phone book, they then examine whether there is a match between the phone number provided in the order details and the phone book. The quote below exemplifies how customers' data are looked up and related to other datasets and how fraud emerges from the combination of the data and personal preferences:

> **There are rarely cases where we do not search for anything. I would cancel something because I don't like the email address, but then I find the name, or I find the customer in a directory, well, in a phone book in France, and then I say okay, the email address is a bit weird, but hadn't I search for it [the email], I would get a ticket [cancel the order] (Agent, 25 Female).**

In addition to Google Search, manual reviewers also frequently access popular social media platforms such as LinkedIn or Facebook to verify customers. Some fraud management tools have a direct link to some of these social media websites, thereby creating a more convenient search option for fraud agents. Social media platforms are usually accessed to find matches between internal and external datasets and also to gain access to additional private and work-related data. For example, while LinkedIn provides insights into the current and past occupations of the customer, Facebook enables manual reviewers to investigate the private aspects of customers,

such as the name of their current partner, and use them to categorise genuine or fraudulent customers.

As an example, one of manual reviewers suspected a customer of fraud because the order details included two different names. As discussed in the previous section, any inconsistencies in the data are labelled as suspicious. However, the order was accepted after viewing the customer's Facebook account, as it displayed the two names emerging in the order details as two people who were in a relationship. In this case, Facebook was considered as the validator. This case also shows that inconsistency in data is not labelled as fraudulent as long as Facebook or any other source can confirm that these two people are related or well-known to each other.

The following quotes show how social media is mobilised by manual reviewers as an external source to verify customers and how reliability and trust are generated through external validators:

> **I mostly find customers on LinkedIn or Xing. These are reliable sources (Agent, 22 Female).**

> **I generally search for the customer. It is very helpful when I find the customer on LinkedIn or Facebook and when I am sure that it is really this person (Agent, 26 Female).**

However, verifying the customer can still be challenging despite the results offered by Google Search or access to social media platforms, because there can be on the one hand many people with the same names and overlapping details, so the order may be related to a person with similar data, and on the other hand customers might not be clearly identified because social media accounts do not always display the real names and identities of users.

Furthermore, a clear verification does not always lead to a positive label:

> **He had different prices, for example five cards for 40 Euros and 15 cards for 100 Euros [The price for stolen credit cards on a fraudulent website] (Agent, 27 Male).**

This quote represents a rather unexceptional case whereby the email address provided in the order details was linked to fraudulent activity on a different website. In this case, the order was labelled as clear fraud and the person was blacklisted so that he could not place any other orders in the future, at least not using the same order details. Nevertheless, "verified" customers are usually considered to be reliable and trustworthy, given that the verification through Google Search or social media accounts often serves as proof that the customer must be who they claim to be.

Furthermore, manual reviewers also frequently use Google Maps as an external resource for accessing additional data. As discussed extensively in Chapter Four, customers living in wealthier areas and in good housing are much more likely to be identified as genuine as opposed to people who live in less wealthy areas, blocks of apartments or areas with a high percentage of ethnic minorities.

> **If I have doubts and such pictures come up, then no chance. Then I cancel and ask customer service to send us tickets to verify him before we lose money. Then he can replace the order and we will release it (Senior Agent, 46 Male).**

As the quote indicates, Google Maps is used to view customers' housing and the areas in which they live, to reinforce the initial categorisation of the customer or to challenge it. In this case, pictures displayed on Google Maps were considered as a support for the initial assessment.

Furthermore, manual reviewers use Google Maps to gather additional data on customers' billing and shipping addresses and use these to categorise them accordingly. Particularly, they examine the distance between the billing and shipping addresses while assigning more trust to customers with a short distance between both addresses. While there is no definition of how small the distance needs to be to be considered genuine, the greater the distance between the two addresses, the more likely customers will be labelled as fraudulent.

Overall, address assessment contributes significantly to customer assessment. Manual reviewers ground their views of good or bad housing and area on the assumption that people living in "good" areas are more likely to have sufficient funds

to make legitimate purchases. While Google images of the housing or area are particularly important, as also previously argued, housing needs to be considered in relation to other datasets and the variations they construct. The following quotes illustrate why Web verification is so important for manual reviewers:

> **We have problems when we can't find customers, which makes it difficult to work. That's reason enough (Agent, 23 Female).**

> **Without it, this process is not possible (Agent, 26 Female).**

Both quotes display the importance of external sources of data with which manual reviewers aim to access more information to make fraud decisions. This means that data that are not generated in the ordering process and do not relate to online transactions are additionally collected and used for fraud examinations. As Kitchin (2014a) previously noted, in these cases the data are repurposed, as fraud agents utilise additional private information for a different purpose.

This practice, however, raises serious ethical concerns, because on the one hand customers are unaware that companies Google them, access their social media accounts, look in phone books and so on and use this information to categorise them as genuine or fraudulent, and on the other hand such methods have discriminatory consequences. However, as Collmann and Matei (2016) point out, ethical concerns are often ignored when performing data-driven practices, which is also reflected in the views of fraud management team members:

> **In this time of global information, you cannot hide anything (Senior Agent, 46 Male).**

> **If somebody cares about data protection, he must keep himself off the internet, or think about what he publishes there (Agent, 55 Female).**

> **No, it is their own information which they themselves put on the internet. It's their own Facebook accounts. They want to be public. I don't see a problem (Project Coordinator, 46 Male).**

Everything that I don't want others to see, I do not put on the internet, and everything on the internet is for the public. […] We only use the information which everyone can see (Team Leader, 33 Male).

I think they also accept being on the internet, because on LinkedIn, they decide themselves to open a LinkedIn account, or a Xing or a Facebook account. They decide themselves to appear in the phone book or not. When you open an account on the internet, you also have to know that that information is accessible to everyone – and really to everyone – for any reason and any purpose (Agent, 22 Female).

Here it is written in the terms and conditions. Your personal data will be checked by a specific bunch of people. If you have problems, do not order with us (Agent, 26 Female).

If we pointed it out at the time of ordering, some customers of course would be scared away (Supervisor, 41 Male).

We enquired about the whole thing. We don't access non-public sources. We also don't summarise the data and capture them in a new database. This means that we only access public sources, to get an image (Client Manager, 38 Male).

There seems to be some consensus amongst the team members that people create accounts on the internet and these can be legitimately accessed for different purposes. Although companies might "inform" customers of their terms and conditions, in that some orders may be declined, customers are not openly informed about the process, and so it seems that questions on data protection and issues of privacy become irrelevant to address. As Friedewald and Pohoryles (2016) point out, an individual's understanding of privacy is shaped and influenced by technology. Google is so essential for fraud management that there is no room for concerns about customer consent or implications of a digital "background check". In fact, the right to privacy could simply mean for the customer that they cannot be verified on the internet, albeit the decision will more than likely result in cancellation. Customers

simply need to provide access to their data and be transparent about who they are, in order to be considered genuine. The next section will examine similarly how phone validation is performed by manual reviewers as the second major external approach of verifying customers through a phone call and then categorising them as either genuine or fraudulent.

5.3.2 Phone Validation

Phone validation represents the final practice of assessing and examining customers. Phone validation is also the only practice where manual reviewers and customers are in direct contact while decisions are made, which means that customers "confirm" whether they are genuine or fraudulent, albeit they are unaware of this process. Phone validation is performed when the decision is still in the balance for fraud agents despite all data-driven assessments, personal or group discussions and access to additional resources.

This approach usually entails confronting the customer with a set of pre-defined questions, while manual reviewers aim to "find out," through the way customer responds, whether they are genuine. The decision results from the fraud agent's perspective on the phone call. The following quote highlights how phone validation can be considered an extension of data-driven fraud assessments, a means of comparison and the final step in fraud assessment:

> **When you have the data, for instance what is customer's name? What mobile number did he give? What email address did he give? Then you can already see a bit, whether the customer looks suspicious. What is the email address? Or does he have a weird name? Too many numbers, or what is his IP address? When I have this data, then I already have an idea what kind of customer we're looking at and what I will ask him on the phone and whether he is perhaps a fraudster or not. Well that already helps, and then what the customer says, whether he has no idea or difficulties while answering (Agent, 27 Male).**

As outlined in the quote, all of the other assessments have been made before the phone call. During the conversation, customers are then expected to "prove" that they are who they claim to be. This procedure is based on the core assumption that while comparing data with the customer, agents will be able to identify a genuine or a fraudulent individual based on the answers provided as well as on the tone of voice; for instance, customers who hesitate or provide inaccurate answers are more likely to be considered fraudulent:

> **This is a decisive criterion, because we think that fraudsters place so many orders and can't necessarily remember whether they bought shoes today but also bought shoes yesterday. I experienced that myself with the phone validation, that people just could not answer or mixed something up. But that's just decisive. Another question is about the items which they bought. When they can answer immediately and perhaps even to talk about the details, such as size and colour, then it's okay (Agent, Male 35).**

> **Honest customers actually always go into it and say then that it is, for instance, it was for the family or for a sports club or something similar. They answer fairly quickly. Fraudsters avoid it (Team Leader, 33 Male).**

Phone validation is grounded on the assumption that genuine customers provide the right information about their order details, while fraudsters cannot provide accurate information or are less likely to do so, given that they might place several orders using other people's personal and transactional data and might not be able to remember all of this information during a phone call. Furthermore, the assumption is also that fraud agents can recognise whether they are genuine through the way customers speak. These are problematic assumptions, because as pointed out earlier, customer behaviour can be very diverse so that it is not possible to divide them easily into two categories.

This is because not all customers can completely remember their order details or are willing to talk on the phone, as this may cause inconvenience, while fraudsters being aware of this process can be well-prepared to answer the questions correctly.

Additionally, in this regard, as discussed in the first section of this chapter, manual reviewers might have varying understandings of suspicious behaviour, which in turn increases the likelihood that they will come to different conclusions based on their own preferences and understandings.

This also becomes clear when considering manual reviewers' selections of orders for phone validation and the choice of questions posed during the phone call. The following quotes exemplify which orders can be chosen and which questions asked by manual reviewers:

> **We have to ask the last four digits of the credit card and if it is the first order to place. We have to ask for the email address. If everything is actually right, and the customer gives a logical answer, we accept it (Agent, 22 Female).**

> **I normally ask whether the customer themselves placed the order. When the order amount is over 1000 Euros, then I ask what it was ordered for or why the amount is so high and for whom it is ordered, etc. (Agent, 23 Female).**

> **I also called when one item was ordered in a big quantity, because I wanted to know what it was meant for (Agent, 55 Female).**

As the quotes show, manual reviewers vary in how they select the orders and the questions they pose, which means this can also lead to varying fraud constructions. Another important point, though, is that while agents can vary in terms of their choices or understandings of unusual or suspicious behaviour, the following quote outlines that the vast majority of orders are indeed accepted after phone validation, regardless of the questions posed by manual reviewers:

> **Customers that are reached, I would say that 95 % are certainly released, and the ones you cancel are often not reached (Team Leader, 33 Male).**

This means that the profiles of genuine or fraudulent customers are constructed not only through the answers they provide, but also simply whether they can be contacted. As the quote outlines, almost all customers contacted via the phone call were labelled as genuine, while customers who could not be reached were much more likely to be labelled as fraudulent regardless of the reason for not being available. This is highlighted further in the following quote:

> **Yes, the management wanted, ordered and left a wrong number, the number was unavailable, well, mistyped. Consequently, the order was blocked [cancelled] due to the suspicion of fraud, and then management called us totally angrily, but this also was sorted (Back Office Team Member, 29 Female).**

As this case shows, the manager of an online retailer was categorised as fraudulent, as the number provided did not work. This is also because the reasons for not being available are usually not examined or taken into much consideration. The following quotes exemplify that phone validation provides manual reviewers very little support in the detection of online fraudsters:

> **Not always. Sometimes, you have cases 50-50. It is your decision to release it or to cancel it. I prefer cancelling it. He can always prove that he is a genuine one afterwards, but if we are wrong, we lose the money for this order, because we won't get the money and the products are gone (Senior Agent, 46 Male).**

> **In my opinion, it is not really helpful. If I placed an order with a stolen credit card and somebody called me, I would say yes, I placed this order. Please release it. It is not very effective, in my opinion, but we still do it (Supervisor, 26 Male).**

> **Of course, it helps when you talk with the customer, once more as a final criterion. As a last decision criterion, it is probably not wrong. But a good fraudster manages that so that you don't have doubts (Supervisor, 41 Male).**

> **There are some calls which are a bit weird. But that has mostly to do with being rude, that they don't want to answer the questions or perhaps they are busy at that point. On the phone, you can't clearly distinguish if they don't want to answer or if they are just busy (Agent, 35 Male).**

As the quotes outline, a clear distinction between genuine and fraudulent customers can remain challenging despite phone validation. While calling a customer can provide agents with some support in their assessment, it will not confirm genuine customers. Ultimately, it remains a subjective process involving various fraud agents with various preferences and values, armed with a selected set of questions and the hope of detecting criminals through this approach. One benefit of phone validation for manual reviewers is that it helps them to justify afterwards the decisions they make. As discussed in Chapter Four, some of the accepted transactions turn into fraud through a chargeback. In such cases, phone validation can then be used as proof that the manual reviewer has taken every step possible to identify the fraudster correctly, but this identification can still fail despite talking personally to the customer.

5.4 Conclusion

This chapter focused on the second sub-question of how online fraud is constructed through social practices, and it discussed how manual reviewers develop a number of internal and external practices to differentiate between genuine and fraudulent customers. While it was examined extensively in Chapter Four that fraud is constructed through generated and assembled datasets, and how they are joined and re-joined, this chapter expanded upon this understanding by exploring how data were utilised within social practices, how additional actors were mobilised and how fraud is constructed in social situations.

It was also argued in the chapter that these practices are developed to overcome the challenge of not knowing the real identity of fraudsters; however, this is a fairly subjective process, because manual reviewers vary in their choice and selection of

orders, preferences and understandings. For this reason, multiple constructions of fraud emerge based on the agent, the orders selected, data searches on the internet, the digital activities of customers, results presented by Google, the accessibility of information, the traceability of online activities, the relatability of datasets, time invested and the suitability of the practice. Furthermore, it was also outlined in the chapter that fraud is a fluid concept, given that the categorisations of genuine or fraudulent customers are not static and can change in line with new data entries, the involvement of customers is based on which manual reviewer examines the case.

The chapter was divided into two main sections. The first section explored individual and collective practices developed by manual reviewers to predict and prevent online fraud. As discussed, manual reviewers make data-driven fraud assessments by examining transactions within a historical context while looking for relations between present cases and past transactions. In this process, assessments of past cases are used in the examination of current transactions. However, as the data can be very diverse and unique, and represent combinations of datasets which were either previously not observed or did not fit into categories based on the examination of past cases, manual reviewers also develop additional practices to support their decision-making.

A popular method amongst manual reviewers is the reliance on one's own feelings, judgement and experience while examining online transactions. This implies that manual reviewers vary in their understandings and preferences concerning online fraud, which in turn means that different results emerge from this practice based on who examines the online transactions and how these are scrutinised. Collective practices are performed similarly and usually involve two or more members of the fraud team, who discuss and negotiate ideas and understandings, eventually proposing a solution. Customers are then categorised as genuine or fraudulent based on which arguments are proposed and given more weight. The final procedure in the first section of this chapter was the cancellation of orders, which is done to provoke an action or to test a customer's reaction. Customers who respond to the cancellation by contacting the customer service centre and filing a complaint are then usually

considered genuine thereafter as opposed to the customer who does not get back to them.

The second part of this chapter explored external practices that require mobilising additional actors to make fraud decisions. The first external practice was Web verification, which refers to searching for personal customer details on the internet while looking for relationships, for example through Google Search or on social media platforms. In this case, manual reviewers look for an external validator who can confirm that the customers are who they say they are. Web searching is also performed to uncover additional information about customers or to view their address and location and use these to construct profiles of genuine and fraudulent customers.

As addressed in the chapter, this raises serious ethical concerns, because on the one hand there is a lack of customer consent to and awareness of this practice, and on the other hand it has discriminatory effects. Customers are not aware that their personal and transactional data are being used for fraud assessments, that they are being Googled, their social media accounts are accessed, or their houses are viewed and that this information is used, even arbitrarily, to define them as good or bad customers.

The final external practice is phone validation, which requires calling a customer personally and confronting them with some questions. The customers are then categorised as genuine or fraudulent based on how they respond, while in most cases the outcome is positive as long as they can be reached.

Christl (2017) argues that data-driven business practices limit the freedom of individuals to make free choices and decisions. While these practices affect individuals and the society at large, they disproportionately target the disadvantaged individuals and groups and contribute to an increase in social inequality. This is also because these practices are kept secret so that it is not possible to have an open and a fair discussion on how such practices could be performed in a fair manner. This proposal does not necessarily contradict corporate objectives given that businesses have a keen interest in the identification of genuine customers and only denying

transactions made by fraudsters. This would nevertheless require that there is an awareness of data-driven social practices and their discriminatory outcomes.

Chapter Four and Chapter Five have discussed expansively how actors such as fraud management team members, technological systems, data, Google, individual and collective social practices and customers come together in the making of online fraud. The next chapter will expand upon these insights by exploring a number of other actors who come into play, and it will examine how online fraud is partly the result of the relationships between several heterogeneous actors.

6. Online Fraud as a Relational Effect

6.1 Introduction

The previous chapters have discussed extensively how online fraud is constructed in relation to people, data and technology. Specifically, it was explored how human actors construct fraud technologies, utilise data and develop social practices, and how all of these come together in the making of online fraud. As discussed in Chapter Two, social constructionism centres on human action, a notion explored empirically in the previous chapters. This chapter will pay greater attention to actor network theory and suggest a broader sense of constructionism which incorporates humans and non-humans rather than prioritising human action. Empirically, this chapter will place the practices of manual reviewers within the broader context of the organisation, namely the customer service centre, which incorporates many human and non-human actors, and explore how human actors such as fraud agents relate to non-humans and how the interplay between them influences how online fraud is constructed. This chapter will address the third sub-research question of how online fraud can be understood as a relational effect.

As discussed in Chapter Two, actor network theory suggests that the world needs to be understood as a relational process – an assemblage of people, things, ideas, organisations, rules and structures – whereby all of these entities come together to construct social realities. This relational process incorporates human and non-human actors without an ontological division between them. Similarly, Belliger and Krieger (2016) point out that organisations are processes that involve heterogeneous human and non-human actors who constantly negotiate and re-negotiate "programs of action" (p.14). While organisations may appear as entities with boundaries and clearly defined rules, they can be considered as an activity negotiating and building actor-networks and making temporary associations with a variety of different actors. As Law (1992) identifies, organisations are always in action and are constantly involved in making and remaking. However, as Nimmo (2011) outlines, organisations cannot be reduced to the relations of human actors, since such relations are enabled, transformed and mediated by a variety of non-humans. As organisations entail a

variety of heterogeneous actors, Latour (2005) suggested that we should follow the actors and identify the traces they leave. By taking this approach, this research follows the members of the fraud management team to trace and unravel their connections to other actors.

Further, Fox (2007) argues that organisations are complex entities that vary in their structure, ideology, culture and style of management. The way organisations are structured, organised or managed has a major impact on how employees communicate, behave and perform their tasks.

For instance, call centres are considered as workplaces with repetitive tasks and highly standardised processes where employees' ability to use their skills are significantly reduced (Connell and Burgess, 2006). Moreover, surveillance is a strong part of call centre work. Call centres use technological tools to keep track of communication with the customers. Particularly, they track how many calls or emails were received and how much time was needed to respond. This is important to on the one hand measure the productivity of the employees and on the other hand whether the pre-defined targets were met (Connell and Burgess, 2006; Sharp, 2003; Russell, 2009).

Furthermore, call centre work is understood as emotional labour, because not only must call centre agents talk with numerous people on the phone throughout their working day, they also regularly deal with unhappy and angry customers who often communicate their dissatisfaction and frustration. While agents aim to help customers with their enquiries and provide a good level of service, being exposed constantly to this form of communication affects their well-being (Lewig and Dollard, 2003).

This chapter will place online fraud within a broader relational perspective and argue that it can be considered an effect of heterogeneous human and non-human actors within multiple networks who constantly interact and negotiate. The aim is to examine how human and non-human actors are assembled in practice (Law and Singleton, 2013), translated into new networks and mobilised to take action. While the previous chapter explored in detail how manual reviewers perform fraud practices, this chapter will also expand upon the understandings developed in the

previous chapter by unravelling the connections and entanglements of manual reviewers and explore how fraud agents do not act on their own; rather, their action is a relational process and is influenced and constrained by other human and non-human actors and the multiple networks in which they are enrolled.

The following chart is a visualisation of the relations between human and non-human actors and actants who are entangled in multiple networks and whose relations are enabled, constrained, mediated and transformed by other actors and actants. The way the actors are assembled and how they connect and re-connect to each other is particularly important, because each variation constructs a particular version of online fraud.

Figure 2. Actor-Networks of Fraud Construction

Source: Author's own

This chapter is divided into three main sections. In the first section, a set of heterogeneous actants are introduced which are assembled within the actor-network of customer service centre. The section discusses how the relations between agents and another set of actants within the customer services influence and constrain the fraud practices explored in the previous chapter.

The second section examines how customer service centres relate to a number of other actor networks that might not be located within the same physical environment but are nevertheless crucial in the making of online fraud. Particularly, it is explored how human actors mobilise or fail to mobilise networks to take action. The final section provides a brief overview of the findings and will set the scene for the next chapter.

6.2 Organisational Actants

This section explores a number of heterogeneous actants within the customer service centre that influence, enable and constrain the previously examined fraud practices. It is argued in this section that social practices need to be understood partly as the effect of the relations of actors within the customer service centre. The term 'actant' is used to show that the actors can be either human or non-human. The following section explores the contracts of agents and how they affect their fraud-related practices.

6.2.1 Agent Contracts

Employee contracts represent the legal basis on which to define a number of roles and responsibilities and to direct agents towards taking particular action. They are the result of organisational interests turned into a text that serves as a framework for the course of action. Within customer services, contracts are constructed in a way that they are particularly flexible so that agents can be assigned multiple roles at the same time, if necessary. Furthermore, contracts can also be considered as the product of joint interest between different actor-networks, such as the service centre and online retailers, as through this legal framework agents can be asked to work for different clients at the same time, work shifts on weekdays and weekends and be moved between projects, if necessary. This is as exemplified in the following quote:

> **Once you are in team and you are not needed, you will be transferred to a different team. The moment we need you, you will come back. At the moment, we have a team of 16 people. Ten are currently working on this project [fraud team]. The other ones are working on other projects at the moment, but they can come back in a minute (Senior Agent, 46 Male).**

As the quote outlines, the contracts are designed in a way that enables fraud agents to handle fraud alongside and in relation to other tasks. This means that they are

mobilised to take multiple roles at the same time, which, as will be explored below, not only constrain their ability to make fraud assessments, but also can create conflicting roles and situations.

6.2.2 Time Constraints

The practices of the fraud agents are also shaped by time constraints which require that fraud-related issues and decisions need to be performed within the "acceptable" time limit. While there are no official documents or legal contracts that define the exact time limit, there is an awareness amongst the agents that they need to finish their fraud assessments within a limited time frame because of the high volume of transactions that need to be reviewed, and sometimes alongside other tasks. As discussed in Chapter Five, agents strive to make the "right" decisions when assessing online orders; however, they can only to do so while taking the time constraints into account, as outlined in the following quotes:

> **Theoretically, we are supposed to be done with an order within 2.30 minutes (Fraud Agent, 26 Female).**

> **We had sales and there were 3,000 orders. Then we did about 2,000 orders in four hours. We had so much time. We were also told we should pay more attention to the quantity rather than quality (Agent, 25 Female).**

> **I think I need at average between 20 seconds and 1 to 1.5 minutes. I would say about one minute on average per day (Team Leader, 33 Male).**

> **In Germany, I need about 30 seconds and in Europe 1.5 minutes (Agent, 26 Female).**

The quotes show clearly that there is an awareness of time limits amongst agents when reviewing online orders. Time limits influence manual reviewers' ability to examine online orders, and so agents might feel pressured to make quick decisions

instead of carrying out a thorough examination. As Chapter Five discussed, the examination of an order can be a long and multi-stepped process, though time constraints can inevitably lead to a process whereby the quantity of examined orders is more important than the quality.

Call centres are structured with the aim of reducing the costs to the minimum while providing customer service. This means that call centres are expected to maximise the level of service they provide such as the volume of calls or emails, while keep the costs at a minimum level (Connell and Burgess, 2006). This applies to fraud examinations as well. Time management becomes a crucial matter for agents when going through online transactions and making fraud decisions.

The quote below exemplifies one respondent's fraud approach that does not meet the requirements of time limitations:

> **But sometimes I have cases where I don't find anything. I then search everything possible and then suddenly 20 minutes gone, and I've still not found anything. That's crazy. When you work on a case you absolutely want to find something and then the time passes, sometimes about 10-20 minutes with special cases (Fraud Agent, 35 Male).**

The quote underlines that agents need to spend a substantial amount of time on some cases, to be completely sure about their decision or to find information they are looking for. This can be tolerable for exceptional cases or when there is a low amount of incoming orders but not as an everyday practice. Unfortunately, this agent's contract was not extended. Even though the reasons for this decision were not communicated, not responding to the time requirement might have played a crucial role.

6.2.3 Training

Training also influences how fraud practices are performed within the customer service centre. The purpose of this training is usually to provide fraud agents with the information they need in order to perform individual fraud examinations. Within the

training process, manual reviewers are shown particularly how to approach orders, what data to focus on, how to search customers' details on the internet and how to make a phone call. However, the training needs to be considered in close relation to the working requirements of the customer service centre which, as pointed out earlier, emphasises the importance of quantity due to the volume of customer enquiries and online transactions. This is also reflected in the training process, which is often of poor quality, because agents often do not receive formal training but learn from their co-workers – in some cases from more senior employees who might be given this additional responsibility beside other daily duties. The following quotes typify how agents are trained to deal with fraud:

> **It was shown to me at that time by S. how the police enquiries need to be done and what we need to pay attention to, and you check that everything is complete, the data that we put together and that's it. Otherwise, we did not have training or anything like that (Team Leader, 26 Female).**

> **Ms H. showed me with what kind of data I must work and how I must process it. It was a one-day induction and then it was okay (Backoffice Team Member, 29 Female).**

As these quotes show, the training can also be rather brief. Furthermore, the training process also implies that knowledge on how to assess fraud and work on police enquiries or any other fraud-related tasks is passed from the senior agents to newcomers, which means that there is a good chance of passing on their views and understandings of fraud to other people who might then develop similar views and understandings. This process is then repeated every time when newcomers arrive. Furthermore, given that the management at the service centre employs many "replaceable" personnel so often, no specific requirements or education are required to be recruited. Instead, knowledge about how to carry out fraud examinations is generated internally through the training process and in relation to other co-workers, which once more emphasises the importance of training, because manual reviewers

then learn through the training process the only “truth” they know in terms of how to decide between genuine and fraudulent customers.

6.2.4 Multiplicity of Tasks and Roles

This section examines how the multiple tasks and roles employees perform at the customer service centre influence their fraud practices and restrain their courses of action. The notion of multiplicity leaves room for tension within customer services, because it means that fraud decisions need to be made alongside many other tasks. Only the “privileged” fraud agents can deal exclusively with fraud detection and prevention, while most other agents have other duties and responsibilities alongside fraud, which means that on the one hand the multiplicity of tasks and roles creates additional pressures for agents, while on the other hand they must prioritise some tasks over others. This can also mean that some tasks will inevitably be neglected or not be given time they might otherwise require.

The necessity of managing a variety of tasks at the same time is generated in conjunction with those online retailers who set specific requirements for the customer service centre. As the main purpose of the service centre is to provide customer support, retailers can set requirements for tasks which are particularly quantifiable. For instance, the retailer can require that x % of calls must be answered within x seconds, or customer emails must be answered within a specific time frame. While requirements for such tasks can be straightforward, fraud is often less defined and not necessarily quantifiable – and often not prioritised. While fraud is undoubtedly an important task in the customer service centre, it is considered no more important than responding to a customer’s phone or email enquiry, even though it is a criminal act.

For this reason, fraud detection and prevention need to be considered in relation to tasks that are present at the customer service centre and the importance of which is defined through their economic value. Prioritising fraud over other tasks could even mean not meeting the target, which in turn can create economic loss. For this reason, there can be less value in emphasising fraud-related tasks, because customer service

is often defined though numbers and statistics rather than fraud management, as outlined below:

> **Well, we have a certain priority here. It's first phone, then email, then tickets [internal enquiries] and then working on the lists, fraud cases, etc. When there is less in the back office, then we work on the fraud cases, but it doesn't have a higher priority (Back Office Team Member, 29 Female).**

> **For us it does not have a very high significance. It is done alongside other tasks (Supervisor, 44 Male).**

> **My major tasks involve everything that is connected to customer service. We give out information to the customers, where exactly their deliveries are. For example, how they place their orders, how we can refund them and also, I do a fraud check if there are any fraudsters around, trying to get lucky (Agent, 21 Male).**

The quotes represent the variety of duties in customer services that are taken care of alongside fraud-related issues while emphasising how fraud management is a normalised practice. As the quotes demonstrate, agents see no difference between an enquiry into a product, for example, and an actual fraud case, while fraud can even be assigned less importance. This occurs also because the multiplicity of tasks, roles and responsibilities creates a conflict for the agents, as they limit the time available to work on each of the defined duties while the responsibilities remain the same. Multiple responsibilities create additional pressures and can reduce the willingness of agents to work additionally on fraud-related cases or to put any extra effort into fraud detection and prevention. This, however, is crucial, particularly for fraud, given that fraud investigations often require to be thorough and to go the extra mile. As discussed extensively in Chapters 4 and 5, fraud assessments are a multistep process which are defined through data. However, the high volume of customer enquiries, additional tasks and pressures can mean that agents might simply be too overwhelmed to do a thorough examination of the data and will instead miss specific details while making fraud decisions.

As an example, I received an email from a Spanish police authority about a fraudulent transaction, asking the customer service centre to provide them with the details of the fraudulent order so that they could carry on with their investigation. While preparing all relevant details of the fraudulent transaction, two more transactions with the same IP address appeared, which were most likely placed by the same person. Perhaps these were not noticed by the police because the fraudster might have used other payment details. However, while details for the requested order were sent to the police, other orders were simply ignored because of the volume of tasks and the limited time available to manage them. As this case shows, the combination of fraud management with other customer service-related tasks makes it more difficult to create a focused fraud assessment. This is also detailed in the quotes below:

> **It is confusing. I am working on Argentina and Mexico. That is quite difficult. In Mexico, the system is not installed properly. It doesn't show the chargeback. We have different lists to check the chargeback. You have to copy this number and search. You have to be really concentrated on that, and then the phone rings. You were like, "Oh, where am I?" It happens to me every time, when I have for example five credit cards, four emails, five different Mexican names and I have to compare, and then the phone rings and the customer wants something. […] Then I forget about the Mexico thing and I have to restart again. I forget it and I have to take all these steps once more and the phone rings once more for the third time and you get back to the big case. For me it is not easy (Agent, 26 Female).**

> **The lines are open from 8 o'clock because there are too few people and that's just a bit difficult (Agent, 24 Male).**

> **Well, the work is fine, in that we can take part in different projects, but doing everything simultaneously doesn't work for me (Agent, 35 Male).**

These quotes illustrate how the multiplicity of tasks creates a challenging situation for the agents, as they must perform fraud management practices with the limited

opportunity to focus extensively on the subject in hand. As the next quote shows, fraud can then become a rather disruptive task, as it takes time away from other "more valuable" responsibilities:

> **Probably not overwhelming, but it's annoying that because of the police requests, many other things are left undone or given to other people, but that's how it is. We must do it and particularly take care of the police. We have noticed when we don't work on police enquiries, soon that they send the second or third reminder (Team leader, 34 Male).**

Furthermore, the fraud-related additional workload can create new pressures and contribute to the stressful working environment. While the possible emergence of this additional pressure can be linked to the interplay between the volume of work, for example the number of incoming phone calls and emails, and the volume of fraud, in many cases there are already existing pressures, in which case managing fraud alongside other duties becomes problematic:

> **Especially at the moment we have a lot of technical issues, hundreds of emails every day and a lot of phone calls, so it does make a difference to have to do this fraud check as well (Agent, 21 Male).**

As the quote shows, agents might already be overwhelmed without the added burden of fraud management. Adding fraud alongside other roles and responsibilities inevitably creates a more challenging working environment.

This section discussed how multiple tasks and responsibilities constrain agents' ability to focus on fraud. While it was argued that their actions need to be considered in relation to the interplay of associations between a variety of organisational actants, the lack of an actant can also be problematic. For example, there are often no organisational rules or regulations which guide agents how to take action when additional fraud-related issues emerge. It is therefore often up to this individual to decide whether they wish to spend additional time to investigate specific cases while being aware that customers might be waiting on the phone. This also means that agents can vary in their willingness to take on additional actions, i.e. while in some

cases an additional investigation will take place, in other cases it will not. This will influence, for example, whether certain fraud cases will go unnoticed. The next section will explore how the back office can positively influence fraud practices.

6.2.5 Back Office

Some employees at the customer service centre work permanently or temporarily in the back office, which means that they focus on their specific tasks and do not need to take any phone calls. This opportunity is particularly welcomed by the agents, as it creates a more comfortable and relaxed working environment. The back office creates a more meaningful and valuable work experience, particularly for agents who take a leading role in fraud management, and can positively influence fraud management practices, because the back office takes the pressure away from being on the phone often with angry customers, responding to some unpleasant emails or doing the same repetitive tasks. For this reason, being in the back office and not having to deal with customers' enquiries can be more rewarding. The following quotes also exemplify how working on fraud, particularly in the back office is valued more than any other customer-related responsibilities or duties:

> **With Vodafone, I did inbound, and I didn't like doing it, to be honest. Here, we work, as you know, only in the back office and work on orders, sometimes also outbound. Yeah, I like this one sort of better (Agent, 23 Female).**

> **The number of deleted and rejected orders will be at a stage where our client will be really proud that we are doing such a good job (Senior Agent, 46 Male).**

> **It is fun, I have to say (Supervisor, 26 Male).**

> **This is quite interesting, because every day you do not copy paste, copy paste. Every day is not the same challenge (Agent, 26 Female).**

It's a task that I like to do. Rather too much than too little (Team Leader, 26 Female).

As these quotes show, agents prefer to do fraud management in the back office, as it strengthens their ability to focus on fraud and reduces additional pressures. However, not all agents can benefit from the back office, as the sole purpose of customer services is to respond to customers' enquiries. This means that most agents must take on multiple roles and responsibilities alongside fraud-related tasks, which inevitably influences how they can do fraud assessments, how much time they can spend and how thorough they can be with their examinations.

This first section of this chapter explored how fraud practices are influenced by a number of actants within the customer service centre. It was argued that while on the one hand the examined actants can create constraints and limitations for fraud practices, on the other hand they can also generate a more positive working environment. The associations between these heterogeneous actants construct different variations of fraud practices, depending on how the bits and pieces come together. However, as entities are constantly involved in making and remaking (Law, 1992), fraud management is never a finished process, and fraud practices are negotiated and changed through associations between various actor networks (Cresswell et al., 2010) such as customer services and retailers.

This means that while some networks may break, other associations are generated. For instance, at the beginning of the research it was observed that agents working for one of the online retailers had a very limited role in handling fraud, mainly passing relevant information between different departments, while towards the end of the research agents were required to take responsibility for manual fraud checks and to make decisions on incoming orders. However, with a different online retailer, it was also observed that agents' fraud-related responsibilities were significantly reduced. This example demonstrates the instability of associations between the actants as well as the fluidity of fraud practices. The next section will explore a set of other actor-networks which are also closely linked to the fraud practices of agents performed within the customer service centre.

6.3 Network Relations of Customer Services

This section will concentrate on the network relations between the customer service centre and other actor-networks and detail how these are assembled, translated and mobilised to take action in relation to fraud. The customer service centre plays a particularly crucial role in assembling many actor-networks, because it is the contact centre for many individual, departmental or organisational enquiries. Furthermore, most of the customer data are assembled here. For this reason, the customer service centre can be considered a significant network relating to several other human and non-human actor-networks such as internal and external departments, organisations and people that collectively construct online fraud through associations between these heterogeneous actor-networks. The following sections will explore network relations between customer services and other entities.

6.3.1 Customer Services

Section 6.2.4 drew on the notion of multiplicity and explored how agents can take multiple roles and responsibilities within different networks. This section will broaden this perspective by considering customer service agents and fraud management agents as two different actor-networks. As Cresswell et al. (2010) point out, organisations can be complex entities consisting of a broad network that can be divided into sub-networks. While both entities are remarkably entangled, network relations can be rather tense and fragile with the specific interests that they impose and negotiate with other entities.

Human actors in the fraud department and in customer services can be considered as two sides of a coin, as each has access to different data and different customer experiences. Customer service's main responsibility is to help customers with their enquiries, to be service-oriented and friendly and build a positive relationship, while the fraud management section aims to detect fraudsters who are disguised as genuine customers. These roles and responsibilities influence both teams' perspective on one another. While customer service agents often consider fraud agents as individuals who cancel "genuine" customers' orders unnecessarily or

without properly assessing their data and create major problems for customers and themselves, fraud agents consider customer service agents as "naive" and easy to deceive, as they fall for the stories of fraudsters while pretending to be good customers.

As these quotes indicate, while both entities are enrolled in the same network through their temporary associations, network relations are constantly negotiated, as both entities are interested in imposing their version of reality about customers. For example, customer service agents have direct contact with customers, so they may feel they are in a better position to judge the situation and then feel fairly frustrated when their views are not taken into consideration, as outlined below:

> **Most of them are pretty annoyed, disappointed and frustrated by what happened with our e-shop. Most of them say in this case I don't see the point in ordering again. We have difficulties on the technical side at the moment – too much frustration because of cancelled orders without a reason (Agent, 21 Male).**

As the quote confirms, the tension is accompanied by other failures such as dysfunctional technology. Nevertheless, customer services agents must deal with frustrated customers who have possibly missed sales or good deals due to the cancellation. Others complain that the order cancellation caused them troubles such as not receiving goods that were needed within a particular time frame or for a particular occasion. While customer service agents can make suggestions for future action, the transaction can be rejected by fraud agents, due to disagreements about the integrity of customers.

This fundamental difference between the fraud and customer services teams creates two different perspectives about customers and leads to a challenging relationship between both entities. Both actor-networks come together, as each can only function fully through the relation of the other; for example, fraud agents cannot be contacted directly by customers. As discussed in Chapter Five, fraud agents frequently cancel customers' orders for a variety of different reasons and also to provoke action. When the customers complain about a cancelled order, they are usually not able to get in

touch with the fraud team directly, so information needs to be circulated from customer services to the fraud team so that they can review customer complaints and take a different action in the future. Furthermore, if the fraud management team wishes to contact the customer, this can also be performed through customer services. From one direction or the other, the circulation of customer enquiries requires the cooperation of both entities.

Nevertheless, the relationship between both entities is rather tense, particularly from the customer services perspective. There are two main reasons for this situation. First, customer services must deal with the consequences of fraud decisions, such as customer reactions to their "unjustifiably" cancelled or delayed orders due to the fraud check. Second, they might often find themselves in a position to explain or justify the decision-making of fraud agents with which they might not agree. This inevitably creates tension, as outlined in the examples below:

> **There was an update a couple of days ago. Suddenly, orders do get cancelled as soon as the external fraud check can't verify a single thing, so as soon as one bit of information can't be verified, they cancel the whole order. It could be that the shipping address varies from the billing address, which is not really sensible because lots of customers order, for example, for their kids, but they just get blocked (Agent, 21 Male).**

> **Online retailers, including the agents, take fraud detection too seriously; for instance, they partly cancel customers' orders because the email address may be slightly suspicious, regardless of the fact that it is the customer's email address they also use to contact us (Team Leader, 26 Female).**

> **Meanwhile, the fraud check is awful. There are orders cancelled which are not supposed to be cancelled (Agent, 58 Female).**

This section focused on the relationship between the fraud department and customer services as two separate actor-networks, and it argued that what counts as online fraud is further shaped by network relations between customer service agents and fraud teams, for instance whether customer enquiries are circulated and how

actors act upon them. This means that the social construction of online fraud is a relational effect between different actor-networks, which is sometimes uncertain, tense and the result of negotiations. The next section will similarly examine another network relation between fraud agents and the warehouse and unravel how this relationship influences what constitutes online fraud.

6.3.2 The Warehouse

Network relations are also configured with the warehouse. While agents communicate with customers regarding their orders, the physical goods purchased by customers are stored and shipped from the warehouse, so there is therefore a close relationship between customer services and the warehouse. Particularly, the alignment between both entities becomes crucial when fraud is suspected after the order has been successfully processed. This can be the case when, for instance, a victim calls in and informs customer services that they have been charged for a purchase that they did not make. In such cases, agents attempt to mobilise employees in the warehouse to stop the shipment. The circulation of information is mediated by internal systems and via a so-called 'ticket', which is a short message. Whether action is taken on suspicious orders is influenced by the workload in the warehouse, whether such information was acknowledged before the shipment leaves the warehouse and whether actors in the warehouse deem it necessary to take action. However, agents also might decide in some cases not to mobilise other actors for the reasons that were discussed above, such as time constraints and multiple roles and responsibilities. This is also a very subjective process, as it varies amongst the agents if and when they should contact the warehouse to stop a shipment.

6.3.3 Shipping Companies

The previous section argued that the shipment can be stopped as long as actors are willing to mobilise other actors to take action. This only works, though, when the products have not yet left the distribution centre. However, once the goods have

been shipped, there is nothing that can be done within customer services or the warehouse to stop the shipment. The only option is to form associations with the shipping companies and mobilise them to take action, by stopping the final delivery and returning the products back to the sender. This process also involves at least two actor-networks, namely the agents who contact the carrier and the carrier itself.

Furthermore, the type of shipping company, the workload and the timing of the circulated message can influence whether the delivery of the goods can be stopped, as exemplified below:

> **Sometimes, DHL is fairly quick. Sometimes, we send an email and a couple of minutes later the answer is, "Yes, we were able to cancel". Sometimes, during the weekend, DHL does not work, which means we send the list there, well we say, "Please cancel this and that", but the response comes basically just on Monday (Agent, 24 Male).**

As the quote outlines, in this case the agent experiences a quick response from DHL. However, in many other cases agents are not able to mobilise delivery companies to take timely action. For example, the carrier may not respond to the message or respond after the goods have been delivered. This can be the case particularly when orders are sent via express delivery. In other cases, the carrier may respond but state that they are unable to help.

Additionally, whether the delivery of goods can be stopped is also influenced by the carrier's own rules and regulations and the existing communication channels between the customer services centre and the carrier, which can work for some but not for others. For instance, we had a customer from Germany who placed an order with a value of about 1000 Euro. Although the order was initially manually assessed and released, communication with the project coordinator cast some doubts about the customer so that we decided to contact the carrier and ask them to return it to the sender. After about 10 minutes on the phone, DHL said that they were not able to help. When they were told that the order cost about 1000 Euro and we believed it was fraud, the person suggested that we should contact the police. However, the police could not be contacted at that stage, because no crime had occurred yet. As

previously argued, it is often not possible factually to know whether a case is fraud. The problem in this instance, though, is that nothing can be done from the fraud management perspective once the products have been delivered.

> **Relatively often we first realise that the order is fraudulent after it has been delivered. Then it is over (Project Coordinator, 46 Male).**

This section explored the significance of alignment between customer services and the carrier, particularly when fraud is suspected after goods have been shipped. As discussed, whether or not entities can be aligned is influenced strongly by the willingness of agents to mobilise other actors. This relates back to the point made earlier that when there is a lack of an actant that can define and distribute roles amongst agents to take action in such a specific case, agents can then decide individually how far they will follow the traces to stop fraud. Additionally, it was identified that the existing communication channels between the customer services and shipping companies, and varying rules and regulations, also influence whether a suspicious order can be stopped successfully. This section shows that the construction of online fraud needs to be considered in relation to the alignment or lack thereof between these entities. Particularly, various constructions are possible based on whether an agent is reporting the case, whether there is an effective reporting mechanism in place, when the fraud case is reported, which shipping company is involved, what the regulations are and how reporting influences shipping companies' own fraud detection and prevention practices. The next section will similarly explore the relationship between customer services and financial institutions.

6.3.4 Financial Institutions

It was discussed in Chapter Four that orders can be automatically rejected by the fraud detection tools of online retailers and also directly by the issuing banks during the transaction, and that both technological tools function in relation to each other. However, as identified in the previous section, some transactions can also be

reported as suspicious or fraudulent after they have been approved by both systems, for example when a victim reports an unauthorised transaction. In such cases, banks are usually informed first, following which these organisations then attempt to mobilise customer service agents to take action and to cancel an order or stop a delivery, as outlined below:

> **We had a case where a credit card institution got in touch and said there are fraud cases related to this credit card. Then we had many customer accounts for that, and we got them blocked (Agent, 24 Male).**

> **Once I was contacted because the bank wanted to have more information because the credit card was used by a fraudster (Supervisor, 26 Male).**

As illustrated in these quotes, the fraud management of financial institutions and online retailers can function in relation to each other. Furthermore, while the previous sections showed that agents usually mobilise other actors to take action, this section makes clear that this is not a one-way street, given that financial institutions attempt to mobilise agents to cancel or stop an order.

This section showed that fraud is constructed partly as the result of the cooperation between both actor-networks. The next section will discuss how police are key actor-networks in terms of reporting fraud cases and how this influences what counts as fraud at the customer service centre.

6.3.5 Police Enquiries

Customer services and police represent two separate actor-networks consisting of many human and non-human actors. However, they also create temporal associations when a police report is filed by a victim of fraud, following which the police usually then contact customer services to acquire information on fraudulent transactions and related datasets, in order to carry out an investigation. Customer services can then either directly circulate the information to the police or send it through to the online retailer, as outlined in quotes below:

> **The police often call us directly. We are basically not allowed to give any information on the phone. Then we ask to send their enquiry via email or mail. Then we forward it completely, as we send it to the fraud department and they take care of everything else (Supervisor, 44 Male).**

> **Once I received an email from an officer and forwarded him all the details, and he requested I give him a call to verify, yeah it is the police, then forwarded him all the details we could find about the order, name, address, where it was collected, how it was paid, etc. Another time the police officer actually called me, and we spoke for about 15 minutes about finding out where the card had been used, the IP address etc., forwarded all the information to them (Agent, 21 Male).**

Both cases demonstrate that the customer service centre is mobilised by the police to take action. Agents play a crucial role in responding to police enquiries, regardless of whether they forward the data personally to the police or to a further department which then contacts the police directly. In both cases, they gather together all possible information about the customer and transaction for the police investigation. Furthermore, there can be other reasons why the police might report a transaction as fraudulent. In addition to the victim's notification, there can also be house searches, for example where fraudulent deliveries can be found and online retailers contacted to receive more information on the delivered goods.

Customer services do not receive the same amount of police notifications for each online retailer. The volume of enquiries varies depending on the retailer, the volume of transactions and the time of year, as shown in the following quote:

> **When you think that the online shop started four years ago, and we had perhaps 30 police enquiries over Christmas. Now we have gone up, I believe 300 or so. It was a lot over the Christmas months (Team Leader, 26 Female).**

This section discussed how police and customer services come together in the making of online fraud. While the police have a key interest in mobilising customer service agents to circulate personal and transactional data used for fraud, police enquiries

influence what constitutes online fraud at the customer service centre, given that the transactions linked to them are usually considered clear fraud cases. However, such cases can be shaped by individual actors such as the agents and their interest in taking further action. As agents often deal with police enquiries on their own initiative, some might inform the fraud departments and mobilise them to block the customer so that no other orders can be placed when using the same or similar data, while others might not be willing to go this extra mile. As previously discussed, fraud-related issues are often not well-defined and regulated at the service centre, which also involves responding to police enquiries. Additionally, this also means that online fraud not only results from whether the police approach customer services, but also how such cases are handled internally and whether they are reported as fraud to the online retailers. This practice is shaped by agents' choices and preferences as well as whether they deem it necessary to spend additional time on fraud examinations.

6.3.6 Fraud Victims

The final actor-network to be explored in this section involves the actual victims of online fraud, who are not considered passive actors but rather people with agency actively shaping what constitutes online fraud. Previous sections detailed how customer services are notified about fraud cases. However, as exemplified in the quote below, in most cases it seems to be the victims who contact the customer service centre and indicate that their personal or payment details have been abused:

> **Up to about 80% of the time, it is really the victims who get in touch (Agent, 29 Female).**

This usually involves people who have detected unauthorised payments in their bank or alternative payment accounts and those affected by identity theft. In many cases, victims get in touch to inform the service centre that they did not make the online payment, or they ask for advice on what to do, particularly when personal data has been abused. The process usually starts with locating the fraudulent transaction in the system, blocking order details and then blacklisting the user so that no other

orders can be placed on the same account. The victims are often advised to take further action by contacting the police.

Furthermore, in many cases, there is multiple victimisation, which means that the payment or personal information of victims have been abused for different purchases, often involving different online retailers. As an example, a lady who was resident in the US contacted me at the customer service centre in Germany indicating that there were charges on her credit card which she did not make, and so she requested a call to discuss the matter. I made two phone calls to resolve the case. During the first call there was no response. However, I soon realised that I did not consider the time difference and that I must have called in the middle of the night in the US. The second attempt was successful, and I was able to talk directly to the victim. Interestingly, the lady seemed to be very calm and relaxed on the phone, as she had previously talked to the bank and was probably able to negotiate a refund. She indicated that there had been other fraudulent transactions such as travel ticket charges. The examination of the case showed that the payment card was abused for an order delivered in the UK, while the payment card was issued in the US and the products were sent from the warehouse in Germany. As this example shows, many national and international actors come together in a fraudulent transaction.

In a different case, a German victim contacted customer services for an unauthorised transaction made using the website of a popular online retailer and insisted that his payment details had been stolen through this website, which for the victim was the only explanation why he had been charged for a purchase he did not make. We looked up his payment details and located the order, which was used for a delivery in Spain, while the cardholder lived in Germany. When the victim repeatedly highlighted that the details were stolen through this website, we asked him whether he had been to Spain previously. He responded that he went there for a holiday and had forgotten all about it. He was recommended to contact the police so that we in turn could provide them with all the necessary documents to carry out an investigation.

Furthermore, victims who contact the customer service centre are often shocked about a crime that has been perpetrated against them. Agents again take on multiple roles and assist customers, as the former are often the first contact point.

This section detailed that fraud victims play a crucial role in the making of online fraud, because many cases are labelled as fraudulent as a result of communication with the people whose transactional or personal data have been abused.

6.4 Conclusion

This chapter centred on the third research question; namely how online fraud can be understood as a relational effect. Fraud practices as discussed in the previous chapters were placed within the wider context of the organisation and organisational relations, while it was explored how human and non-human actors and actor-networks come together in the making of online fraud. In the first part of the chapter, it was argued that fraud practices are influenced and constrained by organisational actants within the customer service centre. Particularly, it was examined how agents' contracts were designed in such a way that agents can be given multiple roles and responsibilities, which, however, create tension and additional pressures and also require that some tasks must be prioritised while others are inevitably neglected. This means that as customer services is rather defined through numbers and statistics, priorities are given to more quantifiable tasks rather than fraud.

The focus on quantity rather than quality is also experienced in the training process, which is rather brief and mainly involves passing the views and understandings of senior agents to newcomers, thus increasing the likelihood of thinking along the same lines and developing similar fraud practices. Furthermore, it was discussed that fraud practices also need to be considered in relation to time constraints, given that agents have a short time frame for fraud decisions, which subsequently influences how thorough they can be with their examinations. These constraints and limitations, however, are less of a problem as long as agents get the opportunity to work in the back office, without having to take phone calls, which in this study was applicable only to a small number of agents.

The second part of the chapter examined the network relations between the customer services centre and other actor-networks and detailed how these are assembled, translated and mobilised to take action. The section started with a discussion on how customer services consist of teams of customer service agents and fraud team agents with varying responsibilities and how this structure creates potential for conflict, because while customer service agents are asked to provide a good service to customers, fraud agents are required to detect fraudulent customers. Tension also exists because in many cases neither cohort knows whether or not the customer is fraudulent. However, decisions made by fraud agents not only have implications for customers, but also for customer service representatives, as such staff are in direct contact with customers and must justify the decisions made by others. It was argued, though, that both teams must align, in order to function.

It was also shown that there are close relations between customer services and other entities such as the warehouse, when attempting to stop a possibly fraudulent order, and shipping companies, who come into play after a product has left the distribution centre. In both cases, agents can mobilise both actor-networks to take action. Furthermore, it was argued that not only agents mobilise others, but they are also mobilised by them. Particularly, specific online orders are labelled as fraudulent by agents as a result of being notified by financial institutions and the police, while it was also outlined that such practices are not well-defined and consequently vary amongst agents. Moreover, the fraud victims were also considered as important actors who significantly shape what cases are categorised as fraud.

Chapter Six explored empirically how online fraud is constructed through the assemblage of multiple actors. The notion of multiplicity implies that there are various ways in which actors can align or fail to align, thereby leading to different fraud constructions. Particularly, it was emphasised that not only fraud agents come into play but many other actors, such as internal rules and regulations, different organisational entities, external companies, police forces and victims. The ongoing relationships between various actor-networks also show that these are constantly involved in the making and remaking of online fraud, which indicates that not only is this a never-ending process, but it is also characterised through tensions,

uncertainties and the fluidity of online fraud. The next chapter will explore two sets of actor-networks, namely retailers and the police, more closely and detail how the network relations between both entities are crucial in the making of online fraud.

7. Actor Networks of Online Retailers

7.1. Introduction

Chapter Six argued that the customer services centre is entangled in heterogeneous relations of humans and non-humans and explored a number of actor-networks that relate to fraud practices in different ways. This chapter will give greater attention to two of these actor-networks, the online retailers and the police who are outside of the customer services, while addressing the final sub-research question of how external actor-networks relate to fraud constructions. Both actor-networks deserve special attention because of their specific relation to fraud management at the customer service centre. As discussed in Chapter One, online retailers often recruit external service providers due to large amounts of customer enquiries which they cannot handle. This also applies to fraud management. While the customer service centre performs manual order review and deals with many other fraud related issues, online retailers define the requirements.

For example, they define roles, targets and the extent and scope of orders to be manually examined which means that fraud agents can only operate within this given framework that has been defined by the online retailer. This is because they are the "owners" of the physical and digital goods while the circulation of goods is the main reason for fraud detection and prevention practices. Further, in Chapter Six it was also discussed that there is a close relation between the customer services and the police as some transactions are labelled as fraudulent after the police notification is received. This chapter will develop this point further by examining the reporting behaviour of retailers and policing of online fraud and how this relates to fraud constructions.

This chapter is divided into two main sections. The first section will focus on online retailers and argue that while online retailers relate to fraud detection practices at the customer service centre, their approach needs to be understood in relation to their structures, capacities, financial constraints, responsibilities and the extent to which fraud is visible to them. The section will show that regardless of whether an agent makes a decision on a single order as explored in Chapter Five, or the manager

of the retailer decides on a bigger scale, for example on how many people need to be mobilised and how high the annual spending can be for fraud prevention and so on. The second section will look at the policing from the perspective of online retailers and the police and will argue that online retailers are reluctant to report fraud cases to the police based on the low chances of investigative success, costs linked to reporting as well as the uncertainty about whether the suspected cases are fraud. However, the lack of reporting on the other hand also influences what is known to police, what forms of fraud can be acted upon and to what extent fraud matters.

In this chapter, the main aim is to explore the last two important actor-networks more closely which have an impact on a larger scale on how online fraud is constructed. The following section will explore how online fraud is experienced by online retailers.

7.2. Fraud Ontologies

This section will explore the fraudulent activities experienced by online retailers and how this relates to the specificities of their retailing model. It will be argued that at least nine out of ten online retailers indicate that they are affected by fraud. Only one online retailer states that they do not have a fraud problem. However, while this retailer has an online website, it only enables customers to make purchases through a sales person who visits the customer in their homes to sign the contract for their high-priced electronic devices. This means that all online retailers with an online website and opportunity to purchase physical or digital goods indicate that they are affected by fraudulent activities, as outlined below:

> **We thought that fraud is a problem in relation to particular retailers, or it depends on whether particular goods are attractive to fraudsters and if these can be resold [through legal or illegal platforms]. We now see the trend with all clients: online fraud occurs whenever the delivery of high-value products is an option (Account Manager, 38 Male).**

While all online retailers seem to be affected by fraud, there can be differences between them. For instance, well-known fashion brands and retailers offering middle to high price products seem to be more strongly associated with fraud as these can re-sold by fraudsters. Further, how an online retailer operates, is also linked to different forms of fraudulent action. For instance, while an online retailer associates fraud with residential addresses, for the other retailer, fraud is related to the delivery of goods to branches in specific cities. As store collection is not offered by the first retailer, they also cannot associate fraud with store deliveries. Similarly, retailers who offer digital goods in the form of downloads, link fraud to digital goods as opposed to the retailers who only provide physical goods.

Moreover, online fraud is not only linked to the abuse of transactional and personal data of others but also to activities of legitimate customers which are made visible through the relations of several actors-networks, such as the customer, the warehouse, customer services, as discussed in the previous chapter. These activities can be detailed as follows:

*Genuine Payment Fraud***:** This refers to transactions which are legitimately made by the customers who claim afterwards that they did not make the purchase. Such cases can be more difficult to examine from the retailer perspective as the below quote outlines:

> **There is clean fraud or friendly fraud, basically you are defrauding the company and you are actually the one placing the order with your credit card, but you say you did not. This is something really hard to detect because it is a single item that he once stole from the shop. It is pretty tough to get rid of in an automated manner (Head of Payment Department, 35).**

Order not received: Some customers claim that their purchases were not successfully delivered to them. Although it is clear that not all orders are successfully delivered as some orders can be lost or damaged during the delivery process or some of the items can go missing when orders include more than one item, it can be difficult from the retailer perspective to know which customers might be making false claims. If the

customer claims that they did not receive the order, the online retailer needs to compensate the customer and return the funds to them even if they have a doubt that the claim might be false.

Returning used items: Such customer activities are not categorised as fraudulent per se; however, these are considered as intentionally harmful.

> **And there are also other frauds. I order clothes and wear them and send them back afterwards and pretend as if I only tried them on. That's also sort of fraud (Supervisor, 41 Male).**

However, in a busy warehouse environment, such cases can often go unnoticed while resending these goods to other customers and shifting the costs of fraud to them. As an example, one of the customers contacted the customer service centre to request a returns label for one of the orders he made but he could not remember his order number. While trying to locate his order in the system and provide him with his returns label, we had to check each and every order he made and compare the details. While doing so, we could see that the customer made several orders within the recent months and almost every order was returned. During the phone conversation, he indicated that he was working for events and that is probably the reason for ordering several pairs of jeans. However, since almost all items were returned after a short time, we wondered whether he was ordering a new pair of trousers for the events every time and returning them afterwards.

After the customer was assisted, we informed the project coordinator about the case. We argued that it was fraud, even though the customer used legitimate payment details. The project coordinator agreed, so we cancelled his next order. When the customer called about the cancellation, we could not provide a valid reason as there are no rules against returning every purchase made so that his next order was accepted.

> **We can't tell the customer we think you are a fraudster (Agent, 24 Male).**

Returning fake items: In another case, we received information from the warehouse regarding several different orders placed in France, often in Paris which were

returned to the warehouse. The warehouse claimed that these customers returned fake products or products which were not purchased in the online store. The first cases were not necessarily questioned, and the products were returned to the customers. However, customers then started calling in and becoming aggressive that they returned the genuine products and are entitled to receive a refund.

In a different case, the customer contacted me and claimed that they received a box with computer components instead of the items they had ordered. I asked the customer to return it and that we will process a refund for them and apologised for the inconvenience. Although it is very unlikely that there are computer parts in the warehouse which were accidently sent to the customer, in many cases the customer is given the benefit of the doubt. This is because there is not clear proof that customer is intentionally misleading the retailer but also because they use social media to raise a complaint which can then cost the company more than refunding an order. Further, in another case an empty box was returned to the warehouse while the customer claimed that all items were in the box when it was given to the carrier. In this case it is very difficult to prove whether it was the customer who returned the box without content or whether the content was removed on the way back to the warehouse or in the warehouse. These examples show that there is a tension between providing a good service and fighting fraud. This goes along with the reputation damage that could occur when strict measures are taken against 'suspicious' customers.

This section showed that almost all retailers state that they have a fraud problem, while their fraud problems vary based on the structure and modelling of their online shop. Further, while fraud is usually linked to the abuse of other people's data, this section extended fraud to some of the activities of legitimate customers. This section shows that fraud is constructed in relation to the specificities of online retailers.

7.3 Varying Approaches to Fraud

In Chapter Five it was detailed that fraud management team members vary in their understandings, preferences and decision-making practices. Similarly, in this section it will be argued that while online retailers can be considered as an entity, a closer

examination shows that they vary in their fraud practices. This is because they operate in relation to other internal and external actants such as resources, capacities and their business allies such as external service providers. As retailers vary in their approach, the framework and structure of fraud management practices also vary amongst them which also influences how fraud is imagined and responded to for example at the service centre. The following quotes exemplify how retailers can vary in their assessments and examination of fraud:

> **I do not want to sound arrogant, but we do have damn merchants or potential clients, basically they don't know what they are doing. They really don't know what they do. […] They just don't want to hear about it. They do not basically believe that this is a big issue (Head of Payment Department, 35 Male).**

> **I only know our client downstairs who indeed implemented a team in his organisation that analyses all payments and refunds and so on (Account Manager, Male 38).**

As the quotes outline, retailers' approach to fraud can be different based on their previous experiences with fraudulent activities, their resources and expertise. As the first quote shows, many retailers might not be aware of online fraud in the first place. Further, retailers can also feel overwhelmed to do an active fraud detection as part of running a business, while many might simply not be prepared for doing a form of online policing. Moreover, while some retailers use advanced fraud detection systems, other retailers make use of basic tools such as an excel sheet to manage fraud which leads to a different course of action as exemplified in the quotes below:

> **We just get a list which are filtered based on categories. There are five to six cities defined which are particularly vulnerable and then we filter vulnerable articles. There is basically no system except Excel (Project Coordinator, 46 Male).**

> **Some try to squeeze out fraud to the maximum, others maybe might not have the best set-up to form the team structure. They are working**

> **on systems that don't allow efficient and quick changes to risk management (Head of Payment Department, 35 Male).**

As the quotes show, fraud is defined and responded to differently amongst the retailers. This means that online fraud is constructed in relation to how fraud is defined through the online retailers, the technologies they use, their experiences and expertise. The next section will explore how fraud practices of online retailers are closely linked to the financial costs.

7.4 Costs and Rationalisations

Online retailers' approach to fraud and the rationalisation of their practices can be understood through their associations with other actants, such as online shopping, cost calculations, external constraints and pressures. The technological development of the internet alongside the rise of the e-commerce industry created a shift from visiting local stores to shopping opportunities through the online shopping websites and platforms, while also generating demands and expectation from the customers such as fast delivery. At the same time, this created new opportunities for fraud, as outlined in the following quote:

> **I believe that it becomes easier to defraud because online shops are based on the comfort of the customer. If you can pay with a credit card with a click, then they do offer it. You place an order today and it is already delivered tomorrow, so everything has become much faster. That opens new opportunities for criminals (Police Officer, 44 Female).**

Online fraud creates a conflicting situation for the retailer that on the one hand aims to provide a positive customer experience and increase sales and on the other hand strives to detect fraud and limit financial losses. Further, not only does fraud cost online retailers but also false positives which refer to the customers who are mistakenly labelled as fraudulent. For this reason, the cost of fraud is fairly crucial in understanding how current fraud management practices are rationalised. The following quotes exemplify the impact of fraud on online retailers:

This year we expect globally for all e-commerce transactions more than 10 billion Euros in fraud associated with cards which is about 0.5 % of card associated volume in e-commerce (Head of Payment Department, 35 Male).

Fraudsters are a small number but have a high impact. 3-4 % of fraud cases can cause damage of 8-10 % (Manager E-Commerce/Payment, Male).

It can really hurt the merchant because you know late after, the fact you have a problem because it is so long until the disputes are coming in from e-consumers (Head of Payment Department, 35 Male).

Moreover, fraud prevention also needs to be added to the costs related to fraud. For example, one of the online retailers spends at least 500.000 Euros annually on fraud prevention, including the recruitment of the manual review team. So not only does fraud cost online retailers but also fraud prevention, as exemplified in the following quote:

The system also costs lots of money. The team for analysis costs a lot of money. The colleagues cost a lot (Account Manager, 38 Male).

Since the beginning of the year only Mexico, we blocked 19,000,000 Pesos. I don't know much that is. It could be millions or a few hundred thousand Euros but still if we don't do fraud check it is very hard to say how much fraud we would get but we could get enormous amounts. We have seen it in the past, it can go up to very high percentages, like 10 % or 20 % of all sales. It can be a very high cost if you do not do this (Payment Director, 39 Male).

Consequently, one of the major objectives of online retailers is to reduce costs of fraud. However, cost is not something static, cost is relational and involves at least two actors such as financial institutions and retailers who can negotiate or challenge it, while attempting to shift the liability to the other side. As discussed in Chapter Five, fraud is also defined through the liability shift between retailers and financial

institutions. However, in most cases the retailer must pay as a result of accepting card payments without the physical existence of the payment card (Montague, 2010).

Furthermore, costs are also generated through the pressures and penalties imposed by the "bigger" actants such as Visa and Mastercard. Financial institutions can impose such demands because credit cards represent a favourable payment method for customers and online retailers need to offer these payment options to make profits. While fraud can already be damaging for the retailer, the regulations of the financial institutions create additional pressures. Consequently, online retailers also have solid interests to reduce fraud due to these consequences as outlined in the quotes below:

> **Merchants are strongly penalised when fraud rates increase (Account Manager, 38 Male).**

> **As a general rule, I would say if we go over 1.5 % chargeback then we have a problem (Payment Director, 39 Male).**

As both quotes highlight, financial institutions have the power to dictate how much fraud online retailers are allowed to have not to get into trouble. While retailers can be fined for high fraud rates, financial institutions can prevent retailers from offering their credit card as a payment method which can be fatal for the retailers, as exemplified in the following quotes:

> **Visa sees every transaction which was processed. They need to protect their name, their brand, their value, and preposition as a pretty safe payment. That is why they make sure that it will not happen and that their brand will not be diminished (Head of Payment Department, 35).**

> **If you continue to have a major issue for a long period of time, then you will get fines and you can lose your right to process Visa and MasterCard (Payment Director, 39 Male).**

At the end they can kick you out, so you are no longer able to process Visa and MasterCard for example (Head of Payment Department, 35 Male).

These quotes make clear that from retailers' perspective it is crucial to keep fraud at a low level to avoid fines and penalties which can burden retailers one-sidedly, in addition to the fraud costs they must already pay.

As examined in this section, almost all online retailers subject to this research are affected by fraud, while fraudulent activities are not necessarily limited to abuse of personal and transactional data of others but also to the activities of legitimate customers. However, as it was discussed, fraud is more difficult to prove when legitimate customers are involved. Further, it was argued that retailers vary in their experience with fraudulent activities based on their business model, the payment and delivery options and the fraud detection tool they use.

As it was outlined, many retailers lack the expertise to deal with fraud as a part of a running a business. Nevertheless, fraud detection and prevention mechanisms are generated because fraud represents a cost factor. This also applies to large and international brands as they also feel pressured by more powerful actors such as major financial institutions to keep the fraud rates low. This means that not only fraudulent transactions are costly for retailers but also additional fines and penalties. The fraud prevention also adds to the costs. This is also because not only does it require the implementation and maintenance of technological tools and additional personnel but also it generates false positives.

This section provided insights into the actor-networks of online retailers. As previously discussed, while online retailers play a crucial role in shaping fraud practices through the customer service centre, this section showed that they are entangled in various relations of their own. This generates a more complex picture because it shows that the chain of actors involved in the making of online fraud goes beyond agents who make fraud decisions on a daily basis and the relations of the customer centre, but includes those who make decisions and shape fraud practices on a larger scale. The next section will examine the relations of online retailers and

the police, while examining how policing can be explored through the associations of both entities.

7.5 Reporting and Policing

This section will focus on reporting practices and policing in relation to online retailers, police forces as well as customers. Particularly, it will be examined how their joint action – or lack of action – leads to a specific form of fraud construction. It will be argued that the lack of reporting by online retailers and customers leads to a reduced rate of fraud cases recorded by the police. In response, the limited action taken by the police in relation to what was reported to them and their priorities, capacities and governmental constraints results in mistrust by online retailers. This reciprocal relation, however, means that both actor-networks cannot align and the network breaks. This may then result in less effective policing practices as well as an increase in fraud rates in the future. The following section will provide crucial insights into the reasons provided by online retailers for not reporting fraud to the police.

7.5.1 Reporting Online Fraud: Retailers

Previous chapters detailed that companies use fraud detection and prevention measurements to limit fraud rates and prevent future victimisation. Nevertheless, while many transactions, in particular chargeback related orders are considered as clear indications of fraud, these are not reported to the police. There is a reluctance to inform the police. The following quotes provide insights into the rationalisation of non-reporting fraud as practiced by online retailers:

> **We don't report them anymore, because it brings nothing. Well, it is good to think that somebody will be re-socialised, but as a company it's not my primary task to re-socialise criminals. As a company it is always a cost-benefit calculation, and when reporting it costs me time, money and trouble and I am invited to attend court hearings where nothing**

> **comes of it, and then I say I will let it be. I believe many companies handle it in the same way (Account Manager, 38 Male).**

> **We don't go after the fraudsters at the moment. If we have a chargeback we do know that it was a fraudster, but we don't go to the police try to get this person arrested. It's not an efficient way for us to manage it at the moment. I want to do it. Other companies definitely do it. We now talk to Europol to do something. I see an opportunity there (Payment Director, 39 Male).**

Two important points are raised in the quotes. First, the lack of reporting is justified through the expected low chances of success given that these were experienced in the previous cases when the initiative was indeed taken to report. Second, as previously explored, cost reduction is one of the main objectives of the online retailer which means that the lack of reporting needs also to be understood in relation to costs that are imposed through the reporting. Costs can occur in different forms, such as financial loss or as loss of time or effort, while retailers seem to have no benefit in investing time into reporting from a financial perspective. Further, filing a police report can also create additional burdens to the company and can require additional personnel or structural changes which can simply add to the already existing costs of being victimised by fraud, as exemplified in the following quotes:

> **I can understand from the perspective of an online shop that they don't want to report the cases to the police. They probably will need to open a department for that (Police Officer, 44 Female).**

> **We have tried it once or twice and it was like a small project for one person to go after one or two cases. It is not worth it (Payment Director, 39 Male).**

> **At the end of the day you need people who deal with it. That can't also be automatized. That must be processed individually (Supervisor, 41 Male).**

As the quotes suggest, reporting will cause companies more trouble than it can help in any way to deal with their fraud problem or limit their financial losses. The next quote shows that retailers might not feel benefited even when exceptionally reported cases lead to an investigation and the police were able to locate the fraudulent people or orders:

> **Well we had a crystal-clear case where 35 or 40 orders were given to an address of a big family and the case was closed because at the end of the day 10 or 12 people pointed at others and claimed that it was them. It was not clear who in fact was responsible which means that there was no conviction because it was not clear. Yes, there was the damage but what do you do with 70 pair of shoes and 65 T-shirts which were worn and are old (Account Manager, 38 Male)?**

While this case could also certainly not be considered as a success for the law enforcement agencies, it is a further example for the retailers that reporting is costly and not beneficial. Further, the lack of reporting needs also to be considered in relation to the complexities and uncertainties of factually determining online fraud. As it was discussed in-depth in previous chapters, fraud decisions are often made on an assumption rather than on clear evidence. Consequently, reporting can be problematic in such cases as outlined in the following quote:

> **There is nothing we do. I don't call the police and say this person at this address is using a credit card. First of all, I can't know for sure. It is enough to make a decision, but I can't call the police and say go and have a look there (Supervisor, 26 Male).**

As the quote exemplifies, reporting is in such cases usually not possible. Additionally, reporting can lead to serious problems for the retailer if they mistakenly label somebody as a fraudster. While such decisions are often made internally, taking it to the court would create a different and more serious dimension. Moreover, the lack of reporting is also influenced by the lack of existing positive relations, trust towards the police and their investigative interests, as outlined in the following quotes:

> **There is no good contact with law enforcement (Payment Director, 39 Male).**

> **We also have to investigate each case which means we can't create a trusting relationship. It doesn't work (Head of Police Department, 56 Male).**

> **Well I must clearly say; the police do not make any effort. It is a victimless offence. There is nobody lying on the ground bleeding. It's a faceless company or faceless corporation that has the damage and that can be paid by the insurance company (Account Manager, 38 Male).**

As the quotes show, there is a tense relation between the police and online retailers. In particular, it seems to be difficult to build a relationship based on mutual trust because on the one hand the objectives of online retailers are different from the objectives of law enforcement, and on the other hand they feel neglected and their interests deprioritised. Nevertheless, retailers may choose to report fraud depending on the damage fraud cases may cause as exemplified in the below quote:

> **It depends on the extent of fraud and on the chances, whether the police will be able to investigate it successfully. It depends on the amount. If it is about 2000-3000 Euros you can report it to the police (Manager E-commerce/Payment).**

This section detailed that online retailers do not report fraud cases to the police for three main reasons. First, the costs that are generated through the reporting, such as financial losses, time, effort and personnel. Second, reporting does not seem to be an option based on the low chances of success. Third, the lack of reporting is related to the complexity of factually determining fraud cases. Further, it was also discussed that there are no established positive and trusting relations between both entities which could be used to build better connections. The lack of reporting is an important issue because, as it also will be explored in the next section, the vast majority of fraud and attempted fraud cases will remain unnoticed by the police and other law enforcement agencies which means that they can only act upon the cases that are

known to them. Consequently, fraud practices of online retailers will also affect how fraud is constructed by the police.

7.5.2 Reporting Online Fraud: Cardholders

In addition to online retailers, customers can also file a police report when their personal or transactional data are used for fraudulent orders. This is because fraud often leads to multiple victimisation including an online retailer that unknowingly accepts a fraudulent transaction while providing the fraudster with digital or physical goods and a person whose data is abused. However, similar to online retailers, customers might also be unwilling to report fraud cases to the police. One of the reasons can be that it is an inconvenient process which takes time and effort. As the following quote underlines, cardholders might also not be aware that there can be more convenient ways to file a police report:

> **The fewest people know that they can do it online and think, they have to go to the police to report it (Supervisor, 41 Male).**

The fraud is usually reported to the bank and the payment card blocked so that the same payment details cannot be used for additional purchases. Customers can then request a refund through chargeback procedures as discussed previously. At this point, perhaps the main difference between online retailers and customers is that customers can easily align with banks to receive their money back, while retailers are required to pay for fraudulent transactions. This also means at the customers' side that there is not necessarily a need to also report it to the police as exemplified in the following quotes:

> **The goodwill of the credit card institutions is quite high. They are not interested that people stop using their credit cards, they also don't want that somebody decides not to use the credit card anymore, so they are willing to pay back (Police Officer, 44 Female).**

> **They get the money back from the bank. Then that's it for them (Payment Director, 39 Male).**

As both quotes indicate, banks and customers have the same objectives to resolve the fraud case so that there is not much room for forwarding them to the police. However, the scenario can be different for the victims, if the bank can prove that the person was negligent with their cards and passwords, as exemplified in the following quotes:

> **If the customer did a mistake, for instance the wallet with the credit card got stolen and ten minutes later cash has been withdrawn. Then everybody knows that the PIN was also inside the wallet. Nobody is so quick to find out (Head of Police Department, 56 Male).**

> **The bank will make clear that it [the behaviour of the customer] is negligent, and they will not pay it. The offender couldn't have taken the money if they did not have the PIN (Police Officer, 44 Female).**

In such cases, customers can be asked to fully cover the costs. Nevertheless, from the police perspective it is crucial that all cases are reported to the police despite the goodwill gestures of financial institutions to resolve the cases on the behalf of their customers, as outlined in the below quote:

> **Most of the victims don't realise that this is a criminal act and maybe there are other people who have been victimised too. They see it from their own point of view. They perhaps lost 250 Euros and got it back. They need to go to the police, give information. That is the time they need to invest to get the money back. But if the financial institution says ok, just sign this. They don't see the way we see it. They don't see that it has to be investigated (Police Officer, 44 Female).**

As addressed in the quote, the importance of reporting can be diminished through the regulations of financial institutions when it involves the transactional details of their customer. However, people can be more willing to report fraud to the police when the identity is abused. This is often the case with open invoice orders whereby

people receive invoices and are asked to pay. As was discussed in Chapter Four, open invoice is a popular payment method in some countries in Europe, particularly in Germany. In such cases, people do not have any allies such as financial institutions to provide support so that they are more likely to get in touch with the police, as exemplified in the quote below:

> **It is also problematic when the personal data was used. Let's say someone places an order using my name and credit card details but gets it delivered somewhere else. It also happens that there is a total identity theft, so their contacts are made under the name. That is very irritating (Police Officer, 44 Female).**

This section focused on the lack of reporting on customers' side while exploring the reasons for not bringing fraud to the attention of the police. It was argued that financial institutions construct easy and convenient ways of dealing with fraud, compensate customers for their losses and shift the cost to the retailers. This is because customers and financial institutions align through common objectives of resolving the fraud case. This also means that from customers' perspective there is often no necessity to file a police report as long as they are compensated. This however, can be different when the identity of customers is abused. The next section will explore fraud from the perspective of the police.

7.5.3 Investigating Online Fraud

This section will focus on policing online fraud. Particularly, it will be explored how police forces investigate online fraud and what the limitations of their work are. In Chapter Five, it was argued that online fraud represents a major challenge for the fraud management team members. Similarly, it is also argued in this section that the complexity of fraud creates a challenge for police forces. This is because in the event of traditional crimes such as burglary or theft, there is usually an immediate victim which can make police investigations more straightforward as opposed to fraud where that victimised individual usually notices fraudulent transactions much later.

The following quote exemplifies the complexities surrounding fraudulent transactions and the chances of investigative success:

> **It depends whether a German company has taken the money, if it is a company abroad and at some point, it ends for German police, it depends how the chances are, if you are lucky, it depends on coincidences. I must also admit that it depends on the person who works on the case. If they have much to do and how deep they can go. The more work you have got, the less time is available for each process (Police Officer, 44 Female).**

As shown in the quote, the police investigations take place in relation to a number of human and non-human actors (location of the retailer, people, time constraints, workload) which jointly influence whether the police are likely to start or carry on with an investigation. The action taken by the police can involve local, national or international actors and their investigative success can be the result of whether these actors can align, as exemplified in the following quotes:

> **The police forces work together, depending on the location of the victim and the offender. We work with the online shops, delivery companies, credit card institutions. There are some who don't answer without having a confirmation from the prosecutor, then it can take a bit longer (Police Officer, 44 Female).**

> **In the UK, although they are our friends, they don't respond if there is a damage below 5000 Euros. If you contact a company in the US and ask them to block a German website, some of them do that to keep their reputation but others are not bothered at all (Head of Police Department, 56 Male).**

> **If you want data from Italy it might take up to 2 years (Head of Police Department, 56 Male).**

> **We work together with banks, for instance when we get information on a parcel agent and suspicion on money laundering and we call the**

> **partner bank where the money should go. They are very helpful. They don't give any information but stop the transaction which is often not the case with Western Union. Mostly, the money is already gone (Head of Police Department, 56 Male).**

As the quotes indicate, police operate in relation to other actors such as companies or banks. The investigations have a lower chance of success when it involves two different countries given that in such cases there can be little or no obligation in responding to police enquiries. Additionally, investigations are influenced by how transactions are managed within an organisation such as Western Union and whether these transactions are traceable. Further, the action taken by the police need to be understood in relation to governmental institutions, judges, laws and bureaucracy. The interplay between them can also be decisive and create constraints, additional procedures to carry on an investigation. For example, the following quote exemplifies that while police can only operate in agreement with the data protection laws, this can also disable them from using available data for investigating fraud related cases.

> **In Germany, the data is only available for a certain time and then deleted, that is also a challenge. The victim says there is the IP but the policy in Germany requires that the police can't access the data. [...] The search for IP is not welcomed by the politicians because there is the freedom to search on the internet whatever they want (Police Officer, 44 Female).**

Moreover, it can also be problematic when the information concerning the same offenders are not centralised but divided between different departments within the police forces, as outlined in the quote below:

> **The centralisation is good in a sense because the offender does not only commit one form of crime. When he does credit card fraud, he does not say "I am going to use only Ebay and credit cards." It could be that I am working on the case of credit card, while my colleague upstairs does the Ebay and somebody else works on it as well at the same time (Police Officer, 44 Female).**

The difficulty of investigating online fraud is also linked to the lack of specialised employees at the police such as computer scientists who have the technical skills to deal with fraud as well as lack of technological tools and devices that can be crucial for the success of the investigation, as addressed in the below quote:

> **With the new crimes we will be always behind because the technology develops so quickly. We cannot equip as quick as mobile phones develop (Head of Police Department, 56 Male).**

The other issue is that even when police track down criminal activities and find actual individuals linked to online crimes, in most cases it is not the actual fraudsters but rather their allies who are detected, for example so-called parcel agents who function as a forwarding service, take fraudulent parcels and send them to a different address or finance agents who make their account available for fraudulent or criminal activities. In most cases, these are also at the same time victims who did not realise that they were part of a criminal act, as exemplified in the quote below:

> **They are very surprised because apparently, they worked for some fake company, they accepted goods and put them into a new a parcel, took pictures of it and send it to this company, for instance send it to Eastern Europe and received money, assuming this is a legal job. Then we say this company does not exist, and you will not receive any money, and this is punishable (Police Officer, 44 Female).**

As these are real and existing people with an address, it can be easier for the police to find them rather than those who place the fraudulent orders. Nevertheless, relating a real name or real person to the crime can already be considered as success in police statistics. The following quote shows that in most cases the real offenders remain undetected:

> **I would say that we successfully investigate less than 5 % of the cases. The statistics do not show the reality. For instance, for phishing attacks, if we can't prove that they are coming from Germany and we can never**

prove them, then they count as international crime which you will not see in the statistics (Head of Police Department, 56 Male).

This section argued that online fraud also represents a challenge for the police. This is because on the one hand there is not an immediate victim and on the other hand because fraud investigations involve many local, national and international actors. These include; retailers, customers, financial institutions, national and international law enforcement agencies, laws, bureaucracy, technological tools and devices and skilled personnel and the investigative success relates to the cooperation between them.

Nevertheless, fraud does not seem to be a priority. This might partly result from the low chances of success; however, it can also be influenced by lack of reporting as addressed in previous sections. As previously argued, police can only act upon fraud cases that are reported or known to them. The years of working experience with the online retailers has shown though that the vast majority of fraudulent transactions remain unreported, which means that the reality of fraud as experienced in police forces will be different from online retailers. This inevitably constructs a particular understanding of fraud and form of practice which might not reflect the level of victimisation experienced amongst online retailers or customers.

7.6 Conclusion

This chapter explored the actor-networks of online retailers and the police while addressing the final sub-research question of how external actor-networks relate to fraud constructions. The chapter consisted of two main sections. The first section focused on online retailers and argued that all online retailers subject to this research are affected by fraud, while fraud is extended to the harmful activities of legitimate customers. Further, it was argued that retailers experience fraud differently based on their business model, the payment and delivery options and the technological tools used for fraud detection. They also vary in their understanding of fraud, the method used for fraud detection while many retailers feel overwhelmed with fraud detection practices given that they often lack knowledge and expertise in fraud prevention and

detection. Nevertheless, they aim to reduce fraud rates because fraud represents a cost factor which not only emerges through fraudulent transactions, chargeback fees, through the fines and penalties imposed by major financial institutions but also through fraud prevention. This section aimed to provide insights into the complexities of fraud practices as performed by the online retailers while suggesting that the chain of actors involved in the making of online fraud goes beyond the customer service centre and includes more powerful actors which might have an impact on a greater scale. While it was discussed in the previous section that online retailers define the framework within which fraud agents can operate, this section shows that online retailers' practices are also relational and constrained by rules and regulations imposed to them.

The second section of this chapter focused on reporting practices and policing online fraud and suggested that there is a lack of reporting amongst the online retailers as well as customers. It was argued that while online retailers are reluctant to report fraud because it requires mobilisation of additional resources which creates additional costs, the customers do not see the necessity to file police reports because they are usually compensated by financial institutions. The lack of reporting is however an important issue given that while fraud already does not seem to be prioritised by the police due to low chances of investigative success, fraudulent activities can be even more neglected because police only act upon cases which are brought to their attention. This means that policing relates to a small number of cases while the vast majority of fraud goes formally and statistically unnoticed and undetected.

8. Conclusions

This research aimed at exploring the complexity of online fraud. This was a journey that started rather unexpectedly, through non-academic work at a customer service centre, which opened up the opportunity for an academic and a more challenging and enriching path. Indeed, this has been a very rewarding and stimulating research experience. In this chapter, the aim is to go back to the main topics of this research and emphasise some of the important elements. This chapter is divided into four main sections. The first section will reiterate the research questions and outline the answers provided throughout this study. The second section will discuss the theoretical, methodological and empirical contributions this thesis makes. The third section will detail the limitations of this research, and the final section will point out the implications of this study for research and practice.

8.1 Answering Research Questions

This work was guided by the main research question: *How is online fraud constructed through social practices and technological and organisational relations?*

The first sub-question was: *How are online customers categorised through their data?* With respect to the first sub-question, it was explored in Chapter Four that the profiles of genuine and fraudulent customers were constructed through automated and manual fraud detection methods and tools relying on digitally generated data. Regarding automated fraud detection, it was observed that the personal and transactional data of customers were captured during the ordering process and were used with the help of algorithmic rules to construct categories of customers. Through a set of pre-defined rules, customers were divided into three groups: good customers, fraudulent customers and those not falling into either of these two groups. Transactions in the final group were sent to the manual review for fraud examination.

Genuineness or suspiciousness was defined solely through manually defined rules implemented into an automated tool, in order to respond to the large number of transactions. It was argued, however, that customers cannot be defined easily

through numbers or rules, given the uniqueness and/or complexity of their behaviour, in which case the manual order review becomes necessary. Automated fraud detection and the manual review system are part of the same process, though, because while automated fraud detection categorises customers and makes selections, the manual order review can re-categorise customers, override algorithmic rules and provide them with a new status affecting their future transactions.

Furthermore, it was examined in detail how customer profiles were constructed through the manual order review. Particularly, it was explored how customers were categorised as genuine or fraudulent based on their data. Within this process, the consistency of data was given a great deal of significance, and so while customers with consistent personal and transactional data were labelled as genuine, customers with unusual combinations or inconsistent datasets were more likely to be labelled the opposite. Moreover, it was shown that customers were defined in relation to specific datasets such as their home address, email address and domain, order value, order frequency, types of products and payment details. The choice of payment method was given specific attention in the manual review process so that customers with safer ways of paying, such as PayPal, bank transfer, prepaid credit cards and American Express, were more likely to be considered genuine, while customers with popular credit cards, such as Visa and Mastercard, were more likely to be labelled as fraudulent.

Similarly, it was explored how customer profiles were constructed in relation to home address, the examination of which was extended to the area, the city, the country and the geographical location of the country within Europe. It was argued that customers living in houses, set in rural or wealthier areas or specific countries in Europe, were more likely to be categorised as genuine, while customers living in big apartment blocks, less-privileged areas and big cities more likely to be labelled as fraudulent. Additionally, the ethnicity and background of customers were also examined as part of the manual order review, while customers with foreign or untypical names were more likely to be labelled as fraudulent. It was stressed, however, that constructions of customer profiles do not usually relate to an

examination of a specific dataset but rather need to be considered in the combination of various datasets. This implied that multiple constructions of fraud in relation to data and technology were possible, based on how data are utilised for fraud assessments and how they are joined and re-joined in the automated and manual processes. Additionally, it was contended that fraud constructions were characterised through fluidity and instability, given that the status of customers could be changed, updated and re-defined, which created a thin line between fraud and non-fraud.

The second sub-question was: *How is online fraud constructed through social practices?* In relation to the research question, it was explored in Chapter Five how manual reviewers develop, maintain and transmit internal and external practices to construct categories of genuine and fraudulent customers. It was argued that manual reviewers utilise data generated in the ordering process to carry out fraud assessments, while data were considered within a historical context. This means that manual reviewers examined customers' personal and transactional data in relation to their previous orders or any other past transactions while looking for relations between present orders and past transactions.

This process required transmitting understandings developed through the past transaction to examine the current case, with the aim of differentiating between genuine and fraudulent customers. However, this practice provided manual reviewers with scant support, given that data can be very diverse and display unique combinations, in which case the development of additional practices becomes necessary. Another popular practice performed by the manual reviewers was their reliance on personal feelings, experience and judgement. Nonetheless, this was a very subjective process, because it went beyond data-driven assessments and included manual reviewers' values, preferences, understandings and interests. This means that while manual reviewers vary in how they examine online orders, this also leads to multiple constructions of fraud.

Fraud examinations were also performed in groups, usually including some members of the fraud team, who would discuss and negotiate ideas and understandings while proposing their version of reality. A fraud decision was then made based on the

arguments presented, which ones were given more weight and whether the manual reviewer agreed with the outcome of the group discussion. When the individual or collective fraud assessment did not result in a clear outcome, the manual reviewer could then decide to cancel the order, to provoke an action or test the customer's reaction. Customers who responded to the cancellation were then usually re-categorised as genuine as opposed to those customers who did not raise their voices.

Additional external practices required moving beyond internal datasets and mobilising supplementary actors. There were two main external practices. The first one included the utilisation of Google, Google Maps, social media platforms and other websites as external validators to confirm the genuineness of the customer. Manual reviewers usually looked up selected customer datasets on the internet, to find matches between the order details and data accessed through other websites, or to find additional data about them. Particularly, social media accounts were accessed to find information, for example, on the profession of customers, while Google Maps was used to view the address and area stated as the customer's home address. Profiles of genuine or fraudulent customers were then constructed based on whether matches could be found, what the additional data could tell about them, how the data were understood and how good or bad the housing might be – all defined individually by the manual reviewers. These practices, however, raised serious ethical concerns, because not only were customers unaware how their data were being repurposed (Kitchin, 2014a) and used for fraud assessments, but they also created categories of inclusion and exclusion (Crawford, 2013) as well as discrimination. The second external practice was phone validation, which entailed contacting customers via a phone call and confronting them with a set of questions, thereafter, categorising them as genuine or fraudulent based on their responses. In this case, customers were usually their own validators, albeit they were totally unaware of this process.

It was argued in Chapter Five that online fraud was constructed in social situations and through the practices and relations of human actors, in addition to data-based fraud constructions addressed previously. Within social practices, the notion of multiplicity surfaced as being particularly important, because fraud practices are

performed individually or in relation to each other, whereby various values, understandings, choices and preferences are negotiated. The varying approaches to fraud, individually or in groups, led to various possibilities as to how fraud can be constructed.

The third research sub-question was: *How can online fraud be understood as a relational effect?* Chapter Six concentrated on this research question and examined how human and non-human actors come together in the making of online fraud. Particularly, it was explored how manual reviewers were entangled in sets of relations through the customer service centre and how fraud practices were enabled and constrained through these relations. It was detailed that agents' contracts were designed in a specific way so that they can be asked to take on multiple roles and responsibilities. While the potential for additional pressures and tensions was created through the requirements defined in the contract, a way of dealing with them was to prioritise some tasks over others, which meant that while quantifiable tasks were given higher priority, fraud was neglected. The focus on quantity rather than on quality was also reflected through the training process, whereby agents were asked to make fraud decisions within a short time frame so that more cases could be examined; however, this influenced how thorough they could be with their fraud examinations. Furthermore, the training process usually involved a senior agent, who guided the newcomer and showed them how to make fraud decisions. As fraud assessment is a subjective process, this meant also that their individual views and understandings were passed onto the new employees, and so there was a good chance that they could develop similar fraud practices.

Moreover, it was also examined how fraud can be understood through the network relations between the customer services centre and other actor-networks. It was argued that customer services consist of teams with varying responsibilities, in this case customer service agents and the fraud team, which creates ground for conflict, because while the former are required to be customer-centric when responding to customers' enquiries, the latter are asked to detect fraudsters who might be disguised as good customers. The conflicting roles agents embody created tension between them because of the contrasting, most often completely opposite, labelling

of customers. Additionally, when fraud agents accept or cancel transactions, customers return to customer service agents, complaining about the issue, which means that in some cases customer service representatives will be asked to justify decisions made by fraud agents with which they might not agree in the first place. Nevertheless, it was argued that both teams need to align in order to function.

Furthermore, there was also a close relationship between the customer services centre and the warehouse, which was important when agents aimed to stop the delivery of suspicious orders. Agents usually attempted to mobilise employees at the warehouse to cancel the shipment when fraud was notified. However, once the parcel had left the warehouse, nothing could be done internally, in which case shipping companies such DHL would be contacted to return the parcel to the sender. In this case, it could depend on the rules and regulations of shipping companies whether a return was possible. Moreover, it was outlined that not all agents might be willing to mobilise these actors to take action, given that the methods for handling such fraud cases were not clearly defined in the customer service centre.

It was also outlined that fraud practices need to be considered in relation to financial institutions, which also contact the customer service centre to cancel a transaction. This usually was the case when a transaction had been initially accepted by the financial institutions who later decided otherwise. In such cases, the involvement of customer service agents was required to cancel the order. Further, police also took a similar approach to the customer service centre to request information on fraudulent orders so that they could carry on with their investigations. Additionally, the victims of fraud were also considered as major actors who notify customer service centres of fraud and strongly shape orders labelled as fraud through the agents. Chapter Six explored empirically how online fraud is constructed through the relations of multiple actor-networks. Particularly, it was outlined that not only human actors come into play, but also non-human actors, who are constantly involved in the ongoing process of making and remaking online fraud.

The final sub-question was: *How do external actor-networks relate to fraud constructions?* In regard to the final research question, it was reasoned in Chapter Seven that fraud practices need to be understood in relation to online retailers and

the police, both of which create an impact on a larger scale. In relation to online retailers, it was detailed that while they define the framework, rules and structures guiding how fraud practices at the service centre are performed, their decisions relate to their own knowledge, understanding and experience of fraud. While almost all online retailers are affected by the issue, they may experience it differently based on their business model, payment and delivery options and methods of fraud detection. Additionally, many retailers lack expertise in this area and feel overwhelmed with the fraud burden, alongside running a business. Nevertheless, fraud detection and prevention measurements are implemented, given that the problem represents costs for retailers.

The costs involved in fraud relate not only to the physical loss of goods, but also to administrative costs and chargeback fees. Additionally, retailers can also be subject to fines and penalties by major financial institutions if their fraud rates are too high. For this reason, they have a keen interest in reducing fraud rates and bringing them down to an acceptable level, which might be also defined through the financial institutions. Fraud prevention, however, also creates costs for online retailers, who need to mobilise additional resources for automated and manual detection, while prevention costs are also related to a loss of revenue through so-called false positives. It was argued that the involvement of online retailers in the fraud practices of agents, and the role of major financial institutions in the fraud practices of retailers, shows that the chain of actors involved in the making of online fraud can be long and somewhat varied.

In addition, it was also examined how fraud practices relate to policing the online fraud. Particularly, it was argued that there is a lack of reporting amongst online retailers as well as customers, because reporting requires online retailers to mobilise additional resources that may generate additional costs, while victimised customers are reluctant to report because they are usually compensated by financial institutions. While financial institutions generate easy and convenient ways for customers to deal with fraud, they usually shift the cost to the online retailers while at the same time reducing the need to file police reports.

Online fraud can also be challenging from the police perspective, because on the one hand there is not an immediately noticeable victim, and on the other hand because fraud investigations involve many local, national and international actors such as retailers, customers, financial institutions, national and international law enforcement agencies, laws, bureaucracy, technological devices and skilled personnel, and the investigative failure and success relate to cooperation between these groups. Nevertheless, reporting represents an important point from the policing perspective, because it means that police can only act upon cases which are known to them, while the vast majority of cases remain unnoticed, which in turn might lead to prioritising other issues. This implies that fraud practices need to be understood in relation to external actors who define the rules, structures and framework of fraud practices on a larger scale. Additionally, policing also relates to these practices in the sense that the lack of reporting leads to particular forms of fraud construction.

8.2. Contributions of the Study

Contribution to Theory

The research was grounded in two theoretical orientations: social constructionism and actor-network theory. In relation to social constructionism, it was argued that it enables a critical lens through which social realities can be explored. Particularly, social constructionism helps to understand how social realities are constructed through social practices, even though these may be taken for granted and experienced as given (Berger and Luckmann, 1966; Burr, 2015).

However, it was also argued that while social constructionism provides a critical theoretical framework, it only explores social realities through human interactions and relations. This approach provides limited support for this study because, as previously discussed, in the event of online fraud there is a technologically mediated form of connectivity between physically separated entities rather than face-to-face interaction. Online fraud is possible because modern technologies enable people to engage with each other while concealing their own identities, helping them remain

anonymous and pretend to be somebody else. This means that online fraud cannot be explored fully without taking the role of the technology into account. Thus, social constructionism cannot fully explain technologically mediated crimes.

The second theoretical orientation was actor network theory, which provides a more holistic approach to fraud whereby the role of non-human actors such as technology, data or organisational relations can also be considered without creating an ontological division between them. This is an important point to reiterate, because online fraud has a cyber and an offline dimension, in that while people might commit crimes within the specific realm of cybercrime, they still have a physical dimension.

This research proposed that we need to develop a different approach to constructionism that takes into account how the social is mediated, enabled and constrained by non-human actors, and to extend the notion of social to non-humans. As investigated throughout this work, online fraud is constructed in relation to data, people, technology, algorithms, rules, regulations, groups, the internet, Google, social media platforms, phone books, customers, contracts, time constraints, back offices, roles and responsibilities, organisational structures and relations, departments, logistics, customer service centres, shipping companies, financial institutions, victims and the police. The assemblage of these human and non-human actors can generate a variety of fraud constructions based on how each actor relates to fraud and how they are connected to, disconnected from and the reconnected with other actors. Furthermore, it was also contended that online fraud does not just happen; rather, it is a fluid concept characterised through tensions, uncertainties and instabilities.

Contribution to the Methodology

It was discussed in the early chapters of this thesis that there is only limited research on online fraud and data-driven practices, because most researchers are either not able to gain access to research sites or lack the expertise to understand how such practices are performed (e.g. Nisbet et al., 2009; Pasquale, 2015; Chan and Moses, 2016).

This research was able to overcome both obstacles and generate in-depth insights into fraud constructions, because it employed a mixed-method approach of semi-structured interviews and auto-ethnography while taking a rather constructionist perspective. While the interviews helped explore the experiences of fraud management team members in depth, the constructionist approach made it possible to go beyond the obvious and look deeper into how online fraud comes into being in otherwise taken-for-granted practices. Furthermore, the holistic perspective made it possible to explore the relations and entanglements of human actors with a number of other human and non-human entities while providing a more complex picture.

Moreover, auto-ethnography was added as a research method because of the researcher's insider status, which perhaps is the most important aspect of this study. As explored, being an insider aided in observing how online fraud was experienced, managed and practiced at the customer service centre. It showed how fraud as a criminal act was normalised and taken for granted, and how this approach was passed onto newcomers without much consideration. Additionally, being an insider also created interest in this specific area of research, thus ensuring more active engagement with fraud or any fraud-related issues and tasks became possible. This in return helped develop a solid foundation (Bailey, 2007) for online fraud as well as a deep understanding of fraud detection tools, technologies and practices. The research process and the depth and breadth of the insights gained through the interviews significantly benefited from the insider position. Insider status also helped recognise how actors were entangled in various activities that influenced the way online fraud practices were performed. This shows that doing research as an insider can contribute significantly to overcoming the difficulties of access as well as developing technical knowledge and understanding of under-researched areas.

Empirical Contributions

It was argued in Chapter Two that while there is much research conducted on some areas of cybercrime, other areas are neglected (Yar, 2013, Owen et al., 2017). Further, it was argued that cybercrime studies have emerged from different disciplines, which shows that studies from computer sciences tend to examine the technical elements

of digital crimes, while social scientists prefer to focus on social aspects (Holt, 2016; Leukfeldt, 2017). This also means that not much attention has been given to human-machine interactions. However, technologically mediated crimes entail both human and non-human actors that need to be considered in order to provide an overall picture. This research showed how a holistic approach at an empirical level was useful, while providing in-depth insights into the human and non-human entities coming together in the making of online fraud. It was also shown not only how human actors or relations are decisive in understanding online fraud, but also how their actions are technologically enabled and mediated.

Additionally, this research provided an exhaustive account of how online fraud is constructed. It was argued that online fraud results from a process of production rather than discovery, which is important, because when the profiles of genuine or fraudulent customers are constructed, these are freed from the circumstances within which they were produced. Furthermore, it was also argued that while online fraud is often taken for granted, there is often a thin line between fraud and non-fraud; rather, it is an unpredictable concept in which the categories of genuine or fraudulent users are frequently negotiated and changed.

Moreover, it was also previously argued that more quantitative studies are required to examine how data-driven practices are performed (Williams and Levi, 2012) and to identify their implications (Kitchin, 2014a). Within this research project, it was investigated how personal and transactional data were used for automated fraud detections and fraud scorings. Furthermore, it was also detailed how people's lives were traced outside their order details, such as through Google Search, Maps and social media accounts, albeit this means that people are scrutinised without their knowledge or consent and are often not able to challenge the way they are labelled.

8.3 Limitations of the Study

As with any other research, this study also has some limitations. First, a closer engagement with its theoretical orientations emerged as a result of empirical insights. This means that, inevitably, some topics became more apparent afterwards,

which could have been explored in the interviews; for example, the interviews did not include any questions on how language was utilised for fraud prevention and detection practices. This happened because qualitative research has an exploratory nature and can lead to results that cannot be anticipated at the beginning of the research. A stronger engagement with the theory prior to the data collection could provide a more detailed understanding on particular aspects.

Second, the study focused mainly on fraud practices at one particular customer service centre. Multiple teams took part in this research and provided insights into their experiences of online fraud. However, as all teams were employed at the same service centre, there is a good chance that their approach to fraud was influenced by the same organisational culture, working conditions and contract agreements, which in turn could then lead to the generation of similar accounts of fraud.

Third, the study provided limited insights into automated fraud detection tools, methods and algorithmic rules. While this research did not aim to explore the automated process to a great extent, it would have been beneficial to gain more insights into how automated tools are constructed.

Fourth, while 32 interviews were conducted overall, only two could be carried out with the police. This also creates limitations on capturing the police perspective on online fraud. Last, there is also the possibility of bias when conducting insider research, which was extensively discussed in Chapter Three, while this is also at the same time one of the main strengths of this study.

8.4 Implications of the Study

This research aimed to engage critically with the fraud management practices of online retailers. The findings have implications for future research, practice and for the members of the study, which will be outlined in this section.

Implications for Research

In general, more qualitative research on online fraud within wider economic, social and technological contexts is required. More specifically, future research could be undertaken to focus on algorithms and human interaction in this regard. While this study provided some insights into the relationship between automated and manual systems, this could be taken further by future work. New studies could also closely examine how the fraud management systems of retailers and banks relate to each other's fraud practices while not necessarily being actively involved in the same process. A stronger focus could also be placed on fraud management practices within neo-liberal markets, to assess how retailers are only small actors within a wider economic world. Another possible area could be a rigorous examination of how online fraud and its prevention are motivated by the consumer culture.

This research also raises some questions for the current criminological discussion on whether crime has moved online. In the light of the findings emerging from this study, future research could focus on the question of how we can measure whether crime has been displaced to cyberspace, while most online fraud remains unrecorded and undetected.

Moreover, when online fraud is not grounded in a legal definition thereof but rather on agents' assessments, what should we then call cancelled or rejected transactions? Are these actual crimes or attempts at crime? How can we define chargeback criminologically? It might be interesting to think about how these practices could be criminologically categorised. For example, when crime is prevented by online retailers, how can these acts be delineated? There is no criminological clarity on these aspects.

Overall, more research in the area of cybercrime and specifically online fraud is required to develop a better understanding between digital economies and technologically mediated crimes.

Implications for Practice

The phrase fraud management evokes a structured or an organised way of handling the issue. However, as this study showed, fraud management can be much more complex, fluid, unstructured and disorganised, can include several linked internal and external actors and can contain errors and limitations based on organisational and economic structures and pressures. The findings support a rigorous examination of fraud practices by online retailers and an awareness of their limitations. Furthermore, the findings also call for social responsibility towards members of the public whose data are used without their consent to perform checks. Additionally, there needs to be awareness of how fraud practices could be discriminatory in relation to the least privileged in society. As Ball (2019) argues there is currently no legal framework to challenge data-driven assessment and categorisations. While inaccurate and faulty scoring models can create significant damage, institutions are not held accountable for their mistakes. This makes these practices a matter of social justice.

Implications for the Public

This study also aimed to raise the awareness of members of the public on how their data are a crucial part of fraud assessment, and to show that customers are scrutinised through their accessible data without their knowledge, in order to make decisions that very often are detrimental to them. People need to be made aware of this issue, because action can only be taken when there is awareness.

This research engaged critically with technologically mediated online fraud, challenged taken-for-granted understandings, unravelled hidden social and data-driven practices and explored the assemblage of human and non-human actors coming together in the making of online fraud.

References

Aas, K. F. (2016). Preface, in Robert, D. and Dufresne, M. (ed.). *Actor-Network Theory and Crime Studies: Explorations in Science and Technology*. Routledge.

Abel, R. (2017). *Russian Cybercriminals Using VOIP Services to Bypass Fraud Verifications* [online]. Available at: https://www.scmagazineuk.com/news/russian-cybercriminals-using-voip-services-to-bypass-fraud-verifications/article/682426/ [Accessed: 14 May 2018].

Action Fraud (2010). *Online Fraud* [online]. Available at: https://www.actionfraud.police.uk/fraud-az-online-fraud [Accessed: 12 May 2018].

Action Fraud (2016). *Online dating fraud cost victims £27 million last year* [online]. Available from: https://www.actionfraud.police.uk/news/online-dating-fraud-cost-victims-27-million-last-year (Accessed 17 February 2019).

Action Fraud (2018). *Victims lost £41 million to romance fraud in 2017* [online]. Available from: https://www.actionfraud.police.uk/news/victims-lost-41-million-to-romance-fraud-in-2017 (Accessed 22 February 2019).

Accenture (2017). *Cost of Cyber Crime Study* [online]. Available at: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf [Accessed: 11 May 2018].

Adams, T. E., Ellis, C. and Jones, S. H. (2016). *Autoethnography: Understanding Qualitative Research*. Oxford University Press.

Adler, P.S., Gay, P.D., Morgan, G. and Reed, M.I. (2014). *The Oxford Handbook of Sociology, Social Theory, and Organization Studies: Contemporary Currents*. Oxford University Press.

Aggarwal, C.C. (2011). An Introduction to Social Network Data Analytics. In: Aggarwal, C. C. (ed.) *Social Network Data Analytics*. Springer US, pp. 1–15. Available at: http://link.springer.com/chapter/10.1007/978-1-4419-8462-3_1 [Accessed: 4 April 2017].

Aghababaei, S. &Makrehchi, M. (2016) Mining Social Media Content for Crime. *International Conference on Web Intelligence (WI)*. October 2016 pp. 526–531.

Akers, R. L. (2013). *Criminological Theories: Introduction and Evaluation*. Routledge.

Akhilomen, J. (2013). Data Mining Application for Cyber Credit-Card Fraud Detection System. In: *Advances in Data Mining. Applications and Theoretical Aspects*. Springer, Berlin, Heidelberg, pp. 218–228. Available at:

https://link.springer.com/chapter/10.1007/978-3-642-39736-3_17 [Accessed: 13 April 2017].

Alcadipani, R. and Hassard, J. (2010). Actor-Network Theory, organizations and critique: towards a politics of organizing. *Organization* [online]. Available at: http://journals.sagepub.com/doi/10.1177/1350508410364441 [Accessed: 25 January 2018].

Almunawar, M.N. (2012). Securing Electronic Transactions to Support E-Commerce. *arXiv:1207.4292 [cs]* [online]. Available at: http://arxiv.org/abs/1207.4292 [Accessed: 23 February 2017].

Amoore, L. and Piotukh, V. (2015). *Algorithmic Life: Calculative Devices in the Age of Big Data.* Routledge.

Andresen, M. & Farrell, G. (2015). *The Criminal Act: The Role and Influence of Routine Activity Theory*. Springer.

Anderson, K.B., Durbin, E. and Salinger, M.A. (2008). Identity Theft. *Journal of Economic Perspectives* 22:171–192.

Anderson, R. (2007). *The Credit Scoring Toolkit: Theory and Practice for Retail Credit Risk Management and Decision Automation.* Oxford University Press.

Andrejevic, M. (2014). Big Data, Big Questions. The Big Data Divide. *International Journal of Communication.* 8:17.

Angouri, J. and Marra, M. (2011). *Constructing Identities at Work*. Springer.

Apptica (2018). *2018 Mobile Fraud Trends* [online]. Available at: https://apptica.com/news/2018-mobile-fraud-trends/ [Accessed: 12 May 2018].

Archer, N., Sproule, S., Yuan, Y., Guo, K. and Xiang, J. (2012). *Identity Theft and Fraud: Evaluating and Managing Risk*. University of Ottawa Press.

Armstrong, G., Giulianotti, R. and Hobbs, D. (2017). *Policing the 2012 London Olympics: Legacy and Social Exclusion*. Routledge.

Arthur, T. (2010). *Actor-Network Theory and Technology Innovation: Advancements and New Concepts: Advancements and New Concepts*. IGI Global.

Arthur, T. (2012). *Social and Professional Applications of Actor-Network Theory for Technology Development*. IGI Global.

Atefeh, F. and Khreich, W. (2015). A Survey of Techniques for Event Detection in Twitter. *Computational Intelligence* 31:132–164.

Athey, S., Catalini, C. and Tucker, C. (2016). *Escaping from Government and*

Corporate Surveillance. Evidence from the MIT Digital Currency Experiment.

Attewell, P. and Monaghan, D. (2015). *Data Mining for the Social Sciences: An Introduction*. Univ of California Press.

Azevedo, J. (1997). *Mapping Reality: An Evolutionary Realist Methodology for the Natural and Social Sciences*. SUNY Press.

Baesens, B., Vlasselaer, V.V. and Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*. John Wiley & Sons.

Baghramian, M. (2011). Constructed Worlds, Contested Truths. In: Schantz, R. and Seidel, M. (eds.) *The Problem of Relativism in the Sociology of (Scientific) Knowledge*. Ontos, pp. 105–130.

Bailey, C.A. (2007). *A Guide to Qualitative Field Research*. Pine Forge Press.

Ball, K. (2019). Blacklists and Black Holes: Credit Scoring in Europe. In Webster, W., and Ball, K. (ed.) *Surveillance and Democracy in Europe*. Routledge.

Bamfield, J. (2012). *Shopping and Crime*. Springer.

Barak, G. (2013). *Media, Process, and the Social Construction of Crime: Studies in Newsmaking Criminology*. Routledge.

Bari, D.A., Chaouchi, M. and Jung, T. (2014). *Predictive Analytics For Dummies*. John Wiley & Sons.

Barkin, J.S. (2003). *Social Construction and the Logic of Money: Financial Predominance and International Economic Leadership*. SUNY Press.

Barnes, B., Bloor, D. and Henry, J. (1996). *Scientific Knowledge: A Sociological Analysis*. A&C Black.

Baron, L.F. and Gomez, R. (2016). *The Associations between Technologies and Societies: The Utility of Actor-Network Theory* [online]. Available at: http://journals.sagepub.com/doi/10.1177/0971721816640615 [Accessed: 25 January 2018].

Bartlett, J. (2015). *The Dark Net: Inside the Digital Underworld*. Melville House.

Bartolacci, M. et al. (2014). Personal Denial of Service (PDOS) Attacks: A Discussion and Exploration of a New Category of Cyber Crime. *Journal of Digital Forensics, Security and Law.* 9(1)

Baumer, E. and Tomlinson, B. (2005). Institutionalization through reciprocal habitualization and typification. In: *Workshop on Radical Agent Concepts*. Springer, pp. 122–134.

BBC (2017). *Scale of cybercrime and fraud revealed* [online]. Available from: https://www.bbc.com/news/uk-38675683 (Accessed 17 February 2019).

Becker, H.S. (2008). *Outsiders*. Simon and Schuster.

Behavior, W. O. & Staff, W. O. B. (2001). *Organizational Studies: Critical Perspectives on Business and Management*. Psychology Press.

Bell, D. and Hollows, J. (2005). *Science, Technology and Culture*. McGraw-Hill Education.

Belliger, A. and Krieger, D.J. (2016). *Organizing Networks: An Actor-Network Theory of Organizations*. transcript Verlag.

Bello-Orgaz, G., Jung, J.J. and Camacho, D. (2016). Social big data: Recent achievements and new challenges. *Information Fusion*28:45–59.

Belo, O., Mota, G. and Fernandes, J. (2016). A Signature Based Method for Fraud Detection on E-Commerce Scenarios. In: *Analysis of Large and Complex Data*. Springer, Cham, pp. 531–543. Available at: https://link.springer.com/chapter/10.1007/978-3-319-25226-1_45 [Accessed: 13 April 2017].

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*. 28, pp 24–31.

Benthall, S. & Haynes, B. D. (2019). Racial categories in machine learning. *Proceedings of the Conference on Fairness, Accountability, and Transparency.* 289–298.

Berg, B.L. and Lune, H. (2012). *Qualitative Research Methods for the Social Sciences*. Pearson.

Berger, P. and Luckmann, T. (1966). *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Doubleday & Company, New York.

Berk, R. (2012). *Criminal Justice Forecasts of Risk: A Machine Learning Approach*. Springer Science & Business Media.

Berry, D.M. (2011). The Computational Turn: Thinking About the Digital Humanities. *Culture Machine* [online]. Available at: http://www.culturemachine.net/index.php/cm/article/view/440 [Accessed: 13

December 2016].

Berthold, M.R., Borgelt, C., Höppner, F. and Klawonn, F. (2010). *Guide to Intelligent Data Analysis: How to Intelligently Make Sense of Real Data*. Springer Science & Business Media.

Bhattacharyya, S., Jha, S., Tharakunnel, K. and Westland, J.C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*50:602–613.

Bijker, W.E. (2016). Do Not Despair: There Is Life after Constructivism. *Science, Technology, & Human Values* [online]. Available at: http://journals.sagepub.com/doi/10.1177/016224399301800107 [Accessed: 25 January 2018].

Bijker, W.E., Hughes, T.P., Pinch, T. and Douglas, D.G. (2012). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. MIT Press.

BKA (2018). *Cybercrime. Handlungsempfehlungen Für Wirtschaftsunternehmen* [online]. Available at: https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/handlungsempfehlungenWirtschaft.pdf [Accessed: 12 May 2018].

Bock, K., Shannon, S., Movahedi, Y. and Cukier, M. (2018). Application of Routine Activity Theory to Cyber Intrusion Location and Time. In: *2017 13th European Dependable Computing Conference (EDCC)*. pp.139–146. Available from: doi.ieeecomputersociety.org/10.1109/EDCC.2017.24 [accessed 22 February 2019].

Boeije, H.R. (2009). *Analysis in Qualitative Research*. SAGE.

Bollier, D. (2010). *The Promise and Peril of Big Data*. Washington, DC: Aspen Institute, Communications and Society Program.

Bolton, R.J. and Hand, D.J. (2002). Statistical Fraud Detection: A Review. *Statistical Science* 17:235–255.

Bolton, R.J., Hand, D.J. and H, D.J. (2001). Unsupervised Profiling Methods for Fraud Detection. In: *Proc. Credit Scoring and Credit Control VII*. pp. 5–7.

Borgman, C.L. (2015). *Big Data, Little Data, No Data: Scholarship in the Networked World*. MIT Press.

Bortfeldt, D.A., Homberger, P.D.J., Kopfer, P.D.H., Pankratz, G. and Strangmeier, D.R. (2008). *Intelligent Decision Support - Intelligente Entscheidungsunterstützung:*

Current Challenges and Approaches - Aktuelle Herausforderungen und Lösungsansätze. Springer Science & Business Media.

Bossler, A. M. & Holt, T. J. (2009). On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*. 3:400-420.

Botterill, D. (2014). Constructionism – A critical realist reply. *Annals of Tourism Research* 48:292–294.

boyd, d. and Crawford, K. (2012). Critical Questions for Big Data. *Information, Communication & Society*15:662–679.

Bradbury, D. (2011). Data mining with LinkedIn. *Computer Fraud & Security* 10:5–8.

Brannick, T. & Coghlan, D. (2007). In Defense of Being "Native": The Case for Insider Academic Research. *Organizational Research Methods*. 10 (1), 59–74.

Bratolacci, R., LeBlanc, L. and Podhradsky, A. (2014). Personal Denial of Service (PDOS) Attacks: A Discussion and Exploration of a New Category of Cyber Crime. *Journal of Digital Forensics, Security and Law* [online]. Available at: https://commons.erau.edu/jdfsl/vol9/iss1/2 [Accessed: 25 January 2019].

Brennan, M. (2016). *Can computers be racist? Big data, inequality, and discrimination* [online]. Available at: https://medium.com/@brennan_mike/can-computers-be-racist-big-data-inequality-and-discrimination-42a8e19cbe6e [Accessed: 16 January 2018].

Brenner, S.W. (2012). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. UPNE.

Breul, J.D. (2017). *Cyber Society, Big Data, and Evaluation: Comparative Policy Evaluation*. Transaction Publishers.

Brignall, M. (2017). *Text Alert: The 'Bank' Message That Cost a Student £5,400 of Her Loan Money | Money | The Guardian* [online]. Available at: https://www.theguardian.com/money/2017/dec/09/text-bank-student-loan-money [Accessed: 25 January 2018].

Brodsky, S.L. and Smitherman, H.O. (2013). *Handbook of Scales for Research in Crime and Delinquency*. Springer Science & Business Media.

Brown, C. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. Forensic Focus - Articles [online]. Available from: https://articles.forensicfocus.com/2015/10/27/investigating-and-prosecuting-

cyber-crime-forensic-dependencies-and-barriers-to-justice/ (Accessed 17 February 2019).

Bruffee, K.A. (1986). Social Construction, Language, and the Authority of Knowledge: A Bibliographical Essay. *College English* 48:773–790.

Brunsson, N. (2007). *The Consequences of Decision-Making*. OUP Oxford.

Bryant, D.R. and Bryant, M.S. (2014). *Policing Digital Crime*. Ashgate Publishing, Ltd.

Bryant, R. (2016). *Policing Digital Crime*. Routledge.

Bühlmann, P., Drineas, P., Kane, M. and Laan, M. van der (2016). *Handbook of Big Data*. CRC Press.

Bumiller, K. (1992). *The Civil Rights Society: The Social Construction of Victims*. JHU Press.

Bunnik, A., Cawley, A., Mulqueen, M. and Zwitter, A. (2016). *Big Data Challenges: Society, Security, Innovation and Ethics*. Springer.

Burgess, J. & Connell, J. (2004). Emerging Developments in Call Centre Research. *Labour & Industry: a journal of the social and economic relations of work*. 14 (3), 1–13.

Burke, R.H. (2013). *An Introduction to Criminological Theory*. Willan.

Burr, V. (1995). *An Introduction to Social Constructionism*. Routledge.

Burr, V. (2003). *Social Constructionism*. Psychology Press.

Burr, V. (2015). *Social Constructionism*. Routledge.

Burrows, R. and Savage, M. (2014). *After the crisis? Big Data and the methodological challenges of empirical sociology.* SAGE.

Busch, L. (2014). Big Data, Big Questions. A Dozen Ways to Get Lost in Translation: Inherent Challenges in Large Scale Data Sets. *International Journal of Communication* 8*:*18.

Bustos, L. (2011). Ecommerce Fraud Management Systems: The What The Why and The How. *Get Elastic Ecommerce Blog* [online]. Available at: https://www.getelastic.com/ecommerce-fraud-management [Accessed: 16 January 2018].

Button, M. (2012) Cross-Border Fraud and the Case for an 'Interfraud'. *Policing: an*

International Journal of Police Strategies & Management, 35: 285-303.

Button, M., Blackbourn, D. and Tunley, M. (2015). 'The Not So Thin Blue Line After All?' Investigative Resources Dedicated to Fighting Fraud/Economic Crime in the United Kingdom. *Policing,* 9: 129-142.

Button, M. & Cross, C. (2017a). *Cyber Frauds, Scams and their Victims*. Taylor & Francis.

Button, M. & Cross, C. (2017b). Technology and fraud: The "Fraudogenic" consequences of the internet revolution, in Mike Maguire & Thomas Holt (eds.) *The Routledge Handbook of Technology, Crime and Justice*. Abingdon, Oxon; New York, NY: Routledge (Taylor & Francis Group).

Button, M. and Tunley, M. (2015). Explaining Fraud Deviancy Attenuation in the United Kingdom. *Crime, Law and Social Change*, 63: 49-64.

Button, M., Lewis, C. and Tapley, J. (2009). *Fraud Typologies and the Victims of Fraud Literature Review*, London: National Fraud Authority.

Cacciottolo, M. & Rees, N. (2017). *Online dating fraud reaches record high* [online]. Available from: https://www.bbc.com/news/uk-38678089 (Accessed 21 February 2019).

Callon, M. (1998). Actor-Network Theory-The Market Test. *Sociological Review - SOCIOL REV* 46:181–195.

Callon, M. (1990). Techno-economic networks and irreversibility. *The Sociological Review* 38:132–161.

Callon, M. and Muniesa, F. (2005). Peripheral Vision: Economic Markets as Calculative Collective Devices. *Organization Studies* 26:1229–1250.

Callon, M., Rip, A. and Law, J. (1986). *Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World*. Springer.

Campbell, N. (2016). *10 eCommerce Fraud Prevention Tools to Stop Fraudsters* [online]. Available at: https://www.templatemonster.com/blog/10-ecommerce-fraud-prevention-tools/ [Accessed: 5 January 2018].

Canali, S. (2016). Big Data, epistemology and causality: Knowledge in and knowledge out in EXPOsOMICS. *Big Data & Society*3:2053951716669530.

Casey, A. (2012). A self-study using action research: changing site expectations and

practice stereotypes. *Educational Action Research* 20:219–232.

Cetina, K.K. and Cicourel, A.V. (2014). *Advances in Social Theory and Methodology (RLE Social Theory): Toward an Integration of Micro- and Macro-Sociologies*. Routledge.

Chan, J. and Moses, L.B. (2016). Is Big Data challenging criminology? *Theoretical Criminology* 20:21–39.

Chang, H. (2016). *Autoethnography as Method*. Routledge.

Chang, H., Hernandez, K. C. And Ngunjiri, F. W. (2016). *Collaborative Autoethnography*. Routledge.

Charmaz, K. (2014). *Constructing Grounded Theory*. SAGE.

Chaudhary, K. and Mallick, B. (2012). *Credit Card Fraud: Bang in E - Commerce - Google-Suche* [online]. Available at: http://www.ijceronline.com/papers/Vol2_issue3/AY023935941.pdf [Accessed: 21 January 2018].

Chaudhary, K. and Mallick, B. (2011). Exploration of Data mining techniques in Fraud Detection: Credit Card. *International Journal of Electronics and Computer Science Engineering* 1:1765–1771.

Chawki, M., Darwish, A., Khan, M.A. and Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer.

Chen, J., Tao, Y., Wang, H. and Chen, T. (2015). Big data based fraud risk management at Alibaba. *The Journal of Finance and Data Science* 1:1–10.

Chen, M. (2014). Is 'Big Data' Actually Reinforcing Social Inequalities? *The Nation* [online]. Available at: https://www.thenation.com/article/big-data-actually-reinforcing-social-inequalities/ [Accessed: 24 January 2018].

Chon, S. & Broadhurst, R. (2014). *Routine Activity Theory and Cybercrime: What about Offender Resources?* [online]. Available from: https://papers.ssrn.com/abstract=2379201 (Accessed 22 February 2019).

Chris, A. (2008). *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete* [online]. Available at: https://www.wired.com/2008/06/pb-theory/ [Accessed: 7 March 2017].

Christie, N. (2004). *A Suitable Amount of Crime*. Psychology Press.

Christina, A. (2010). *Personal Data Privacy and Protection in a Surveillance Era:*

Technologies and Practices: Technologies and Practices. IGI Global.

Christl, W. (2017). *How Companies Use Personal Data Against People*. Cracked Labs.

Christl, W. and Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Cracked Labs.

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Springer.

Ciancaglini,V., Balduzzi, M., Goncharov, M., McArdle, R. (2014). *Deep Web und Cybercrime. Nichtallein TOR* [online]. Available at: http://www.trendmicro.de/media/wp/deep-web-and-cybercrime-wp-de.pdf [Accessed: 11 May 2018].

Cifas (2009). *The Anonymous Attacker. A Special Report on Identity Fraud and Account Takeover* [online]. Available at: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/The_Anonymous_Attacker_CIFAS_Special_Report_Oct_2009.pdf [Accessed: 12 May 2018].

Cifas (2018). *Fraudscape 2018* [online]. Available from: https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2018 (Accessed 17 February 2019).

City of London Police (2016). *Cyber Crime - Victimology Analysis* [online]. Available from: https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf (Accessed 17 February 2019).

City of London Police (2017). *One victim reports dating fraud every three hours according to the latest national figures from City of London Police* [online]. Available from: http://news.cityoflondon.police.uk/r/757/one_victim_reports_dating_fraud_every_three_hours (Accessed 17 February 2019).

City of London Police (2018). *Festive fraud: Christmas shoppers urged to stay safe online as victims were defrauded of over £11 million in 2017/18* [online]. Available from: http://news.cityoflondon.police.uk/r/1150/festive_fraud__christmas_shoppers_urged_to_stay_s (Accessed 17 February 2019).

CIOReview (2015). *PayPal's Fight against Fraud with Predictive Analysis* [online]. Available at: http://www.cioreview.com/news/paypal-s-fight-against-fraud-with-predictive-analysis-nid-15227-cid-21.html [Accessed: 18 April 2017].

Clarke, R. (1988). *Information Technology and Dataveillance*. Available from: http://www.rogerclarke.com/DV/CACM88.html (Accessed 17 February 2019).

Clarke, R. and Felson, M. (2004). Introduction: Criminology, Routine Activity and Rational Choice. In: Lambert, R. (ed.) *Routine Activity and Rational Choice, Volume 5*. Transaction Publishers.

Claypoole, T. and Payton, T. (2016). *Protecting Your Internet Identity: Are You Naked Online?* Rowman & Littlefield.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Coghlan, D. and Brannick, T. (2014). *Doing Action Research in Your Own Organization*. SAGE.

Cohen, L. E. and Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*. 44 (4), 588–608.

Coles, B. (2015). A 'Suitable Person': an 'insider' perspective. *British Journal of Learning Disabilities*43.

Collmann, J. and Matei, S.A. (2016). *Ethical Reasoning in Big Data: An Exploratory Analysis*. Springer.

Connell, J. and Burgess, J. (2006). *Developments in the Call Centre Industry: Analysis, Changes and Challenges*. Routledge.

Copes, H. and Vieraitis, L.M. (2012). *Identity Thieves: Motives and Methods*. UPNE.

Cornish, D. and Clarke, R. (2002). Crime as a Rational Choice. In: Cote, S. (ed.) *Criminological Theories: Bridging the Past to the Future*. Sage Publications.

Cornish, D. B. & Clarke, R. V. (2014). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Transaction Publishers.

Costley, C., Elliott, G.C. and Gibbs, P. (2010). *Doing Work Based Research: Approaches to Enquiry for Insider-Researchers*. SAGE.

Cote, S. (2002). *Criminological Theories: Bridging the Past to the Future*. Chronicle Books.

Couldry, N. and Mejias, U. A. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*.

Cowls, J. (2014). Big Data, Ethics, and the Social Implications of Knowledge Production. *Josh Cowls* [online]. Available at:

https://joshcowls.com/2014/08/26/big-data-ethics-and-the-social-implications-of-knowledge-production/ [Accessed: 20 December 2016].

Craig, T. and Ludloff, M. (2011). *Privacy and Big Data*. O'Reilly Media, Inc.

Crawford, K. (2013). *The Hidden Biases in Big Data* [online]. Available at: https://hbr.org/2013/04/the-hidden-biases-in-big-data [Accessed: 12 December 2016].

Crawford, K., Miltner, K. and Gray, M.L. (2014). Critiquing Big Data: Politics, Ethics, Epistemology. *International Journal of Communication* 8:1663–1672.

Cresswell, K.M., Worth, A. and Sheikh, A. (2010). Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare. *BMC Medical Informatics and Decision Making* 10:67.

Crossley, M., Arthur, L. and McNess, E. (2015). *Revisiting Insider-Outsider Research in Comparative and International Education*. Symposium Books Ltd.

Crowther, D. and Green, M. (2004). *Organisational Theory*. CIPD Publishing.

Curry, S. (2000). *An Inside Look at E-Commerce Fraud* [online]. Available at: https://www.scambusters.org/ecommercefraud.pdf [Accessed: 16 January 2018].

Custers, B., Calders, T., Schermer, B. and Zarsky, T. (2012). *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*. Springer Science & Business Media.

Czabanski, J. (2008). *Estimates of Cost of Crime: History, Methodologies, and Implications*. Springer Science & Business Media.

Damri, L. (2016). *E-Commerce Fraud Predictions for 2017* [online]. Available at: https://www.digitalcommerce360.com/2016/10/20/e-commerce-fraud-predictions-2017/ [Accessed: 23 September 2017].

Daniels, J. and Gregory, K. (2016). *Digital Sociology in Everyday Life*. Policy Press.

Dankert, R. (2011). *Using Actor-Network Theory (ANT) doing research* [online]. Available at: https://ritskedankert.nl/using-actor-network-theory-ant-doing-research/ [Accessed: 25 January 2018].

Daws, R. (2014). *London Police Using Big Data to Tackle Small Crime* [online]. Available at: https://www.cloudcomputing-news.net/news/2014/oct/31/london-police-using-big-data-tackle-small-crime/ [Accessed: 24 January 2018].

Delamaire, L., Abdou, H. and Pointon, J. (2009). Credit card fraud and detection

techniques: a review. *Banks and Bank systems* 4:57–68.

Deloitte Development LLC (2015). *Cyber risk in retail. Protecting the retail business to secure tomorrow's growth* [online]. Available at: https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/risk/cl-ers-retail-cyber-risk-report.pdf [Accessed: 11 May 2018].

Demeritt, D. (2002). What is the 'social construction of nature'? A typology and sympathetic critique. *Progress in Human Geography* 26:767–790.

Demery, P. (2009). *How Urban Outfitters Speeds through Manual Review of Payment Transactions* [online]. Available at: https://www.internetretailer.com/2009/09/16/how-urban-outfitters-speeds-through-manual-review-of-payment-tra [Accessed: 21 December 2016].

Denshire, S. (2014). On Auto-Ethnography. *Current Sociology Review*. 62(6): pp. 831-850.

Diaz-Leon, E. (2015). What Is Social Construction? *European Journal of Philosophy.*23:1137–1152.

Diefenbach, T. (2013). *Hierarchy and Organisation: Toward a General Theory of Hierarchical Social Systems*. Routledge.

Diesner, J. (2015). Small decisions with big impact on data analytics. *Big Data & Society.*2, 2053951715617185.

Distil Networks (2018).*2018 Bad Bot Report* [online]. Available from: https://resources.distilnetworks.com/travel/2018-bad-bot-report (Accessed 1 March 2019).

Dolwick, J.S. (2009). 'The Social' and Beyond: Introducing Actor-Network Theory. *Journal of Maritime Archaeology*4:21–49.

Douglas, D.G. (2012). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Bijker, W. E., Hughes, T. P. and Pinch, T. (eds.). MIT Press. Available at: http://www.jstor.org/stable/j.ctt5vjrsq [Accessed: 25 January 2018].

Dowling, S. (2013). *Cyber crime: a review of the evidence* [online]. Available from: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence (Accessed 17 February 2019).

Dua, S. and Du, X. (2016). *Data Mining and Machine Learning in Cybersecurity*. CRC Press.

Dudhwala, F. (n.d.). *What is Actor-Network Theory?* [online]. Available from: https://www.academia.edu/542543/What_is_Actor-Network_Theory (Accessed 8 March 2019).

Dupont, B. (2008). Hacking the panopticon: Distributed online surveillance and resistance, in *Surveillance and Governance: Crime Control and Beyond*. Sociology of Crime, Law and Deviance. Emerald Group Publishing Limited. pp. 257–278.

Durepos, G. and Mills, A.J. (2012). Actor-Network Theory, ANTi-History and critical organizational historiography. *Organization* 19:703–721.

Dutton, W.H. (2013). *The Oxford Handbook of Internet Studies*. OUP Oxford.

Dwyer, S. C. & Buckle, J. L. (2009). The Space Between: On Being an Insider-Outsider in Qualitative Research. *International Journal of Qualitative Methods*. 8 (1), 54–63.

Earle, R. (2014). Insider and Out: Making Sense of a Prison Experience and a Research Experience. *Qualitative Inquiry*20:429–438.

Ebbers, M., Chintala, D.R., Ranjan, P., Sreenivasan, L. and Redbooks, I.B.M. (2013). *Real-Time Fraud Detection Analytics on IBM System Z*. IBM Redbooks.

Economist Intelligence Unit (2012). *The Deciding Factor: Big Data & Decision Making.* [online]. Available at: https://www.capgemini.com/resources/the-deciding-factor-big-data-decision-making/ [Accessed: 13 July 2018].

Edley, N. (2001). Unravelling social constructionism. *Theory and Psychology* 11:433–441.

Edwards, Ashmore and Potter (1995). Death and Furniture: The Rhetoric, Politics and Theology of Bottom Line Arguments against Relativism. *ResearchGate* 8:25–49.

Eglin, P. and Hester, S. (2013). *A Sociology of Crime*. Routledge.

Elder-Vass, D. (2008). Searching for realism, structure and agency in Actor Network Theory1: Searching for realism, structure and agency in Actor Network Theory. *The British Journal of Sociology*. 59 (3), 455–473.

Elder-Vass, D. (2012). *The Reality of Social Construction*. Cambridge University Press.

Eldridge, J. E. T. & Crombie, A. D. (2013). *A Sociology of Organisations (RLE: Organizations)*. Routledge.

Elmer, G., Langlois, G. and Redden, J. (2015). *Compromised Data: From Social Media to Big Data*. Bloomsbury Publishing USA.

Epston, D. (2014). Ethnography, Co-research and Insider Knowledges. *Australian and New Zealand Journal of Family Therapy* 35:105–109.

Eriksson, L. (2011). *Rational Choice Theory: Potential and Limits*. Macmillan International Higher Education.

Esposti, S. D. (2014). When big data meets dataveillance: the hidden side of analytics. *Surveillance & Society*. 12 (2), 209–225.

Europol (2018). *141 arrested in worldwide crackdown on airline fraud* [online]. Available from: https://www.europol.europa.eu/newsroom/news/141-arrested-in-worldwide-crackdown-airline-fraud (Accessed 1 March 2019).

Everett, C. (2015). Big data – the future of cyber-security or its latest threat? *Computer Fraud & Security* 2015:14–17.

Experian (2018). *Global Fraud Report 2018* [online]. Available from: http://www.experian.com/decision-analytics/global-fraud-report-2018.html (Accessed 17 February 2019).

Experian (2018). The 2018 *Global Fraud Report and Identity Report. Exploring the links between customer recognition, convenience, trust and fraud risk* [online]. Available at: https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf [Accessed: 12 May 2018].

Fairhurst, G.T. and Grant, D. (2010). The Social Construction of Leadership: A Sailing Guide. *Management Communication Quarterly*24:171–210.

Feltner, T. & Heller, D. (2015). *High Price of Mandatory Auto Insurance in Predominantly African American Communities*. 16.

Fenwick, T. and Edwards, R. (2012). *Researching Education Through Actor-Network Theory*. John Wiley & Sons.

Ferguson, A.G. (2014). *Big Data and Predictive Reasonable Suspicion*. Rochester, NY: Social Science Research Network. Available at: https://papers.ssrn.com/abstract=2394683 [Accessed: 12 December 2016].

Ferretti, F.F. (2006). Re-thinking the regulatory environment of credit reporting: Could legislation stem privacy and discrimination concerns? *Journal of Financial Regulation and Compliance*14:254–272.

Filipe, J. and Obaidat, M.S. (2008). *E-Business and Telecommunications: 4th International Conference, ICETE 2007, Barcelona, Spain, July 28-31, 2007, Revised Selected Papers*. Springer Science & Business Media.

Financial Fraud Action UK (2017). *Fraud the Facts 2017. The Definitive Overview of Payment Industry Fraud* [online]. Available at: https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf [Accessed: 12 May 2018].

Finlay, S. (2014). *Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods*. Springer.

Finlay, S. (2010). *The Management of Consumer Credit: Theory and Practice*. Springer.

Fisher, D., Hogan, B., Brush, A.J., Smith, M.A. and Jacobs, A. (2006). Using Social Sorting to Enhance Email Management. , 1 January 2006. Available from: https://www.microsoft.com/en-us/research/publication/using-social-sorting-to-enhance-email-management/ [accessed 24 February 2019].

Fleetwood, J. and Potter, G.R. (2017). Ethnographic research on crime and control: Editors' introduction. *Methodological Innovations*10:2059799117728859.

Flick, U. (2014). *An Introduction to Qualitative Research*. SAGE.

Flick, U. (2013). *The SAGE Handbook of Qualitative Data Analysis*. SAGE.

Floyd, A. and Arthur, L. (2012). Researching from within: external and internal ethical engagement. *International Journal of Research & Method in Education*35:171–180.

Floyd, J. (2015). *Immediate Need for Fraud Prevention* [online]. Available at: https://www.aciworldwide.com/insights/expert-view/2015/september/immediate-need-for-fraud-prevention [Accessed: 16 January 2018].

Fox, W. (2007). *Managing Organisational Behaviour*. Juta and Company Ltd.

Fraud Advisory Panel (2016). *In 2006 The Fraud Review talked of an anti-fraud culture throughout society based on deterrence, prevention, detection, investing* [online]. Available from: https://www.fraudadvisorypanel.org/wp-content/uploads/2016/06/The-Fraud-Review-Ten-Years-On-WEB.pdf (Accessed 9 March 2019).

FraudWatch International (2017). What is… a Romance Scam? Don't get fooled by Valentine's Day fever! [online] Available at: https://fraudwatchinternational.com/expert-explanations/romance-scam-valentines-day/

Friedewald, M. and Pohoryles, R.J. (2016). *Privacy and Security in the Digital Age:*

Privacy in the Age of Super-Technologies. Routledge.

Friedrichs, D.O. (2007). Transnational Crime and Global Criminology: Definitional, Typological, and Contextual Conundrums. *Social Justice*34:4–18.

Galbin, A. (2014). An introduction to social constructionism. *Social Research Reports*26:82.

Galletta, A. (2013). *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication*. NYU Press.

Gandy, O.H. (1993). *The Panoptic Sort: A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries* [online]. Westview Press, Inc.

Gandy, O.H. (1996). Coming to Terms with the Panoptic Sort, in Lyon, D. and Zureik, E. (ed.). *Computers, Surveillance, and Privacy*. University of Minnesota Press, pp. 132-155.

Gandy, O.H. (2017). Surveillance and the Formation of Public Policy. *Surveillance & Society*. 15 (1), 158–171.

Gergen, K.J. (2001). *Social Construction in Context*. SAGE.

Gergen, K.J. and Gergen, M. (2003). *Social Construction: A Reader*. SAGE.

Gergen, K.J. (2009). *Realities and Relationships: Soundings in Social Construction*. Harvard University Press.

Gergen, K.J. and Davis, K.E. (2012). *The Social Construction of the Person*. Springer Science & Business Media.

Gergen, K.J. (2015). *An Invitation to Social Construction*. SAGE.

Gestel, T.V. and Baesens, B. (2008). *Credit Risk Management: Basic Concepts: Financial Risk Components, Rating Analysis, Models, Economic and Regulatory Capital*. OUP Oxford.

Get Safe Online (2016). *Fraud & cybercrime cost UK nearly £11bn in past year* [online]. Available from: https://www.getsafeonline.org/news/fraud-cybercrime-cost-uk-nearly-11bn-in-past-year/ (Accessed 17 February 2019).

Ghernaouti-Helie, S. (2016). *Cyber Power: Crime, Conflict and Security in Cyberspace*. CRC Press.

Ghosh, A.K. (2012). *E-Commerce Security and Privacy*. Springer Science & Business

Media.

Gibbs, G.R. (2008). *Analysing Qualitative Data*. SAGE.

Gigerenzer, G. (2014). *Risk Savvy: How to Make Good Decisions*. Penguin Publishing Group.

Gill, M. (2004). Preventing Money Laundering or Obstructing Business?: Financial Companies' Perspectives on 'Know Your Customer' Procedures. *British Journal of Criminology*. 44 (4), 582–594.

Gill, M. (2007). The Challenges for the Security Sector: Thinking About Security Research. *Security Journal; London*. 20 (1), 27–29.

Gill, M. (2015). Senior police officers' perspectives on private security: sceptics, pragmatists and embracers. *Policing and Society*. 25 (3), 276–293.

Gill, M. (2016). *The Handbook of Security*. Springer.

Gill, M. and Hart, J. (1997). Policing as a business: The organisation and structure of private investigation. *Policing and Society*. 7 (2), 117–141.

Gitelman, L. (ed.) (2013). *'Raw Data' Is an Oxymoron*. The MIT Press.

Given, L.M. (2015). *100 Questions (and Answers) About Qualitative Research*. SAGE Publications.

Glucksmann, M. A. (2004). Call configurations: varieties of call centre and divisions of labour. *Work, Employment and Society*. 18 (4), 795–811.

Godfrey, B.S., Lawrence, P. and Williams, C.A. (2007). *History and Crime*. SAGE.

Goode, E. and Ben-Yehuda, N. (2010). *Moral Panics: The Social Construction of Deviance*. John Wiley & Sons.

Goodman, M. (2015). *Future Crimes: Inside The Digital Underground and the Battle For Our Connected World*. Random House.

Goodman, S.E. and Sofaer, A.D. (2001). *The Transnational Dimension of Cyber Crime and Terrorism*. First Printing edition. Stanford, CA: Hoover Institution Press.

Grabosky, P. (2006). *Electronic Crime*. 1 edition. Upper Saddle River, N.J: Prentice Hall.

Grabosky, P. and Smith, R. (2003). *Digital Crime in the Twenty-First Century,* in David S. Wall (ed.), *Cyberspace Crime*, Ashgate Publishing Ltd, Aldershot, UK, pp. 39-57.

Graham, S.D.N. (2005). Software-sorted geographies. *Progress in Human Geography*29:562–580.

Greene, M. (2014). *On the Inside Looking In: Methodological Insights and Challenges in Conducting Qualitative Insider Research. The Qualitative Report*. 19 (29), 1–13.

Gregoriou, C. (2012). *Constructing Crime: Discourse and Cultural Representations of Crime and 'Deviance'*. Springer.

Gregory, M. and Glance, D. (2014). *Security and the Networked Society*. Springer Science & Business Media.

Grimmer, J. (2015). We Are All Social Scientists Now: How Big Data, Machine Learning, and Causal Inference Work Together. *PS: Political Science & Politics*48:80–83.

Grint, K. (2005). *The Sociology of Work: Introduction*. Polity.

Grint, K. and Woolgar, S. (1995). On some failures of nerve in constructivist and feminist analyses of technology. *Science, Technology, & Human Values*20:286–310.

Guide, E. (2017). Ecommerce Fraud Guide - How to detect ecommerce fraud & prevent? *Ecommerce Guide* [online]. Available at: /guides/ecommerce-fraud/ [Accessed: 25 January 2018].

Hacking, I. (1992). Review of Science in Action: How to Follow Scientists and Engineers through Society. The Pasteurization of France. *Philosophy of Science*59:510–512.

Hacking, I. (1999). *The Social Construction of What?* Harvard University Press.

Haggerty, K. D. and Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology*. 51 (4), 605–622.

Haggerty, K. D. (2004). Technology and crime policy: Reply to Michael Jacobson. *Theoretical Criminology*. 8 (4), 491–497.

Haggerty, K.D., Wilson, D. and Smith, G.J.D. (2011). Theorizing surveillance in crime control. *Theoretical Criminology*, 15(3), pp.231–237.

Hakikur, R. (2009). *Social and Political Implications of Data Mining: Knowledge Management in E-Government: Knowledge Management in E-Government*. IGI Global.

Hale, C., Hayward, K., Wahidin, A. and Wincup, E. (2013). *Criminology*. OUP Oxford.

Hall, S. and Winlow, S. (2015). *Revitalizing Criminological Theory: Towards a New Ultra-Realism*. 1 edition. Routledge.

Hammersley, M. and Traianou, A. (2012). *Ethics in Qualitative Research: Controversies and Contexts*. SAGE.

Han, J., Pei, J. and Kamber, M. (2006). *Data Mining, Southeast Asia Edition*. Morgan Kaufmann.

Hans Radder (1992). Normative Reflexions on Constructivist Approaches to Science and Technology. *Social Studies of Science*22:141–173.

Harcourt, B.E. (2008). *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. University of Chicago Press.

Harding, J. (2013). *Qualitative Data Analysis from Start to Finish*. SAGE.

Hardy, M.A. and Bryman, A. (2009). *Handbook of Data Analysis*. SAGE.

Harford, T. (2014). Big data: A big mistake? *Significance*11:14–19.

Hecker, A. (2012). Knowledge Beyond the Individual? Making Sense of a Notion of Collective Knowledge in Organization Theory. *Organization Studies*. 33 (3), 423–445.

Hedenus, A. and Backman, C. (2017). Explaining the Data Double: Confessions and Self-Examinations in Job Recruitments. *Surveillance & Society*. 15 (5), 640–654.

Helbing, D. (2015). *Thinking Ahead - Essays on Big Data, Digital Revolution, and Participatory Market Society*. Springer.

Henry, S. (2009). Social Construction of Crime. In: *21st Century Criminology: A Reference Handbook*. SAGE Publications, Inc., pp. 296–304. Available at: http://sk.sagepub.com/reference/criminology/n34.xml [Accessed: 15 July 2017].

Herlyn, G. (2014). Passagierdifferenzierung als Social Sorting – Anmerkungen zur Diskussion um zukünftige Sicherheitsmaßnahmen am Flughafen aus kulturwissenschaftlicher Sicht. In: Wagner, K. and Bonss, W. (ed.) *Risiko basiert vs One Size fits all*. SIRA.

Hern, A. (2018). Cybercrime: £130bn stolen from consumers in 2017, report says. *The Guardian* [online]. Available at: http://www.theguardian.com/technology/2018/jan/23/cybercrime-130bn-stolen-consumers-2017-report-victims-phishing-ransomware-online-hacking [Accessed: 26 May 2018].

heise online (2017). *BKA: Über 51 Millionen Euro Schaden durch Cybercrime*

[online]. Available at: https://www.heise.de/newsticker/meldung/BKA-Ueber-51-Millionen-Euro-Schaden-durch-Cybercrime-3702465.html [Accessed: 12 May 2018].

Hibberd, F.J. (2005). *Unfolding Social Constructionism*. Springer Science & Business Media.

Hier, S. P. (2003). Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes of social control. *Surveillance & Society*. 1 (3), 399–411.

Hill, J.B. and Marion, N.E. (2016). *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century: Computer Crimes, Laws, and Policing in the 21st Century*. ABC-CLIO.

Hine, C. (2015). *Ethnography for the Internet: Embedded, Embodied and Everyday*. Bloomsbury Publishing.

Hjelm, T. (2014). *Social Constructionisms: Approaches to the Study of the Human World*. Palgrave Macmillan.

Holstein, J.A. and Gubrium, J.F. (2008). *Handbook of Constructionist Research*. Guilford Press.

Holt, T. J. (2012). Examining the Forces Shaping Cybercrime Markets Online: *Social Science Computer Review* [online]. Available from: https://journals.sagepub.com/doi/pdf/10.1177/0894439312452998 (Accessed 17 February 2019).

Holt, T.J. (2016). *Cybercrime Through an Interdisciplinary Lens*. Routledge.

Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C. (2017). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Holtgrewe, U. and Kerst, C. (2002). *Call Center: Die Institutionalisierung von Flexibilität*. *Industrielle Beziehungen*. 23.

Hosking, D.M. (2011). Telling Tales of Relations: Appreciating Relational Constructionism. *ResearchGate* [online]. Available at: https://www.researchgate.net/publication/228714653_Telling_Tales_of_Relations_Appreciating_Relational_Constructionism [Accessed: 21 December 2016].

Hosking, D.M. and McNamee, S. (2006). *The Social Construction of Organization*. Liber.

Howard, R. (2009). *Cyber Fraud: Tactics, Techniques and Procedures*. CRC Press.

Howells, T. (2016). *Supervised Machine Learning 101: The Accurate Way to Make Predictions* [online]. Available at: https://www.fraudtechwire.com/supervised-machine-learning-101-the-accurate-way-to-make-predictions/ [Accessed: 17 April 2017].

Hsieh, M.-L. and Wang, S.-Y. K. (2018). *Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree* [online]. Available from: https://works.bepress.com/shun-yung-kevin-wang/23/ (Accessed 22 February 2019).

Hu, F. (2016). *Big Data: Storage, Sharing, and Security*. CRC Press.

Huber, E. and Pospisil, B. (2018). *Die Cyber-Kriminellen in Wien: Eine Analyse von 2006-2016*. Edition-Donau-Univ. Krems.

Humphrey, C. (2007). Insider-outsider: Activating the hyphen. *Action Research*5:11–26.

Humphrey, C. (2012). Dilemmas in doing insider research in professional education. *Qualitative Social Work* [online]. Available at: http://journals.sagepub.com/doi/10.1177/1473325012446006 [Accessed: 25 January 2018].

Hutchings, A. (2018). Leaving on a jet plane: the trade in fraudulently obtained airline tickets. *Crime, Law and Social Change*. 70 (4), 461–487.

Hutchings, A. and Hayes, H. (2010). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the "Net"? *Current Issues in Criminal Justice: Vol 20, No 3*. Available from: https://www.tandfonline.com/doi/abs/10.1080/10345329.2009.12035821 [accessed 10 July 2019].

Imre, A. (2016). *TV Socialism*. Durham: Duke University Press.

Introna, L. and Wood, D. (2002). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*2.

Ioannidis, J.P.A. (2005). Why Most Published Research Findings Are False.*PLoS Medicine*2:124.

Iphofen, R. (2009). *Ethical Decision Making in Social Research: A Practical Guide*. Palgrave Macmillan.

ITU Telecommunication Development Bureau (2012). *Understanding cybercrime: Phenomena, challenges and legal response* [online]. Available at:

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf [Accessed: 11 May 2018].

Jabri, M. (2017). *Managing Organizational Change: Process, Social Construction and Dialogue*. Macmillan Education UK.

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press.

Jansen, J. and Stol, W.PH. (ed.) (2013). *Offenders in a digitized society* [online]. Available at https://www.researchgate.net/publication/280096971_Offenders_in_a_digitized_society (Accessed 22 February 2019).

Japkowicz, N. and Stefanowski, J. (2015). *Big Data Analysis: New Algorithms for a New Society*. Springer.

Jewkes, Y. and Yar, M. (2013). *Handbook of Internet Crime*. Routledge.

John, P. (2017). *Field Experiments in Political Science and Public Policy: Practical Lessons in Design and Delivery*. Routledge.

Johnson, M. (2013). *Cyber Crime, Security and Digital Intelligence*. Gower Publishing, Ltd.

Jones, K. M. L. (2018). *What is a data double?* Data Doubles [online]. Available from: http://datadoubles.org/2018/05/01/what-is-a-data-double/ (Accessed 22 February 2019).

Juniper Research (2016). *Online Payment Fraud Whitepaper 2016 – 2020* [online]. Available at: https://www.experian.com/assets/decision-analytics/white-papers/juniper-research-online-payment-fraud-wp-2016.pdf [Accessed: 12 May 2018].

Kaptelinin, V. and Nardi, B.A. (2009). *Acting with Technology: Activity Theory and Interaction Design*. MIT Press.

Kelley, A. (2014). Layers of consciousness: An autoethnographic study of the comprehensive exam process. *International Journal of Doctoral Studies.* 9, 347-360.

Khan, A. (2015). Bitcoin – payment method or fraud prevention tool? *Computer Fraud & Security*2015:16–19.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime

Countries. *Social Science Computer Review*. 30 (4), 470–486.

King, N. and Horrocks, C. (2010). *Interviews in Qualitative Research*. SAGE.

Kirwan, G. and Power, A. (2013). *Cybercrime: The Psychology of Online Offenders*. Cambridge University Press.

Kitchin, R. (2014a). Big Data, new epistemologies and paradigm shifts. *Big Data & Society*1:2053951714528481.

Kitchin, R. (2014b). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. SAGE.

Kitchin, R. (2014c). The real-time city? Big data and smart urbanism. *GeoJournal*79:1–14.

Kitchin, R. and Dodge, M. (2011). *Code/Space: Software and Everyday Life*. MIT Press.

Klecuń, E. (2004). Conducting Critical Research in Information Systems: Can Actor-Network Theory Help? In: Kaplan, B., Truex, D. P., Wastell, D., Wood-Harper, A. T. and DeGross, J. I. (eds.) *Information Systems Research*. Boston: Kluwer Academic Publishers, pp. 259–274. Available at: http://link.springer.com/10.1007/1-4020-8095-6_15 [Accessed: 25 January 2018].

Knorr-Cetina, K. (1981). *The Manufacture of Knowledge: An Essay on the Constructivist and Contextual Nature of Science*. Pergamon Press.

Koch, A.M. (2005). *Knowledge and Social Construction*. Lexington Books.

Konsument Europa (2014). *Chargeback within the EU/EEA – a Possibility to Recover Your Money - Konsument Europa* [online]. Available at: http://www.konsumenteuropa.se/en/news-and-press-releases/pressmeddelanden/press-releases-2014/chargeback-within-the-EU-EEA-a-possibility-to-recover-your-money/ [Accessed: 16 January 2018].

Kostopoulos, G. (2017). *Cyberspace and Cybersecurity, Second Edition*. CRC Press.

KPMG International (2016). *Global profiles of the fraudster 2016* [online]. Available from: https://home.kpmg/xx/en/home/insights/2016/05/profiles-of-the-fraudster-an-illustrative-look-at-the-findings.html (Accessed 17 February 2019).

Kremling, J. and Parker, A.M.S. (2017). *Cyberspace, Cybersecurity, and Cybercrime*. SAGE Publications.

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and*

Strategic Perspectives. Springer Science & Business Media.

Kudyba, S. (2014). *Big Data, Mining, and Analytics: Components of Strategic Decision Making*. CRC Press.

Lagesen, V.A. (2012). Reassembling gender: Actor-network theory (ANT) and the making of the technology in gender. *Social Studies of Science* [online]. Available at: http://journals.sagepub.com/doi/10.1177/0306312712437078 [Accessed: 25 January 2018].

Lambert, R. D. (2017). *Routine Activity and Rational Choice*. Routledge.

Langlois, G., Redden, J. and Elmer, G. (2015). Introduction: Compromised Data - From Social Media to Big Data, in Elmer, G., Langlois, G. and Redden, J. (ed.) *Compromised data: from social media to big data*. New York: Bloomsbury Publication Inc, pp. 1-11.

Lam, D. (2014). *Big Data Challenges in Social Sciences & Humanities Research* [online]. Available at: https://www.datanami.com/2014/09/08/big-data-challenges-social-sciences-humanities-research/ [Accessed: 16 January 2018].

Lamers, M.H. and Verbeek, F.J. (2011). *Human-Robot Personal Relationships: Third International Conference, HRPR 2010, Leiden, The Netherlands, June 23-24, 2010, Revised Selected Papers*. Springer Science & Business Media.

Lantzsch, K., Altmeppen, K.-D. and Will, A. (2010). *Handbuch Unterhaltungsproduktion: Beschaffung und Produktion von Fernsehunterhaltung*. Springer-Verlag.

Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers Through Society*. Harvard University Press.

Latour, B. (1990). Technology is Society made Durable. In: *The Sociological Review*. pp. 103–131.

Latour, B. (1992). *Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts* [online]. Available at: http://www.bruno-latour.fr/node/258 [Accessed: 15 July 2017].

Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Mass: Harvard University Press.

Latour, B. (1996). *On actor-network theory: A few clarifications.* Soziale Welt, 47(4), 367, 369–381.

Latour, B. (2000). When things strike back: a possible contribution of 'science studies' to the social sciences. *The British Journal of Sociology*51:107–123.

Latour, B. (2004). Why has critique run out of steam? From matters of fact to matters of concern. *Critical inquiry*30:225–248.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press.

Latour, B. (2010). Tarde's idea of quantification. *The Social after Gabriel Tarde: Debates and Assessments*, 1 January 2010, pp.145–162.

Latour, B. and Woolgar, S. (1979). *Laboratory Life: The Construction of Scientific Facts*. Beverly Hills, Sage Publications.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems practice*5:379–393.

Law, J. (2004). After Method: Mess in Social Science Research. Routledge.

Law, J. (2008). Actor Network Theory and Material Semiotics. In: Turner, B.S. (ed.) (2009) *The New Blackwell Companion to Social Theory*. Wiley-Blackwell, pp. 141–158. Available at: http://onlinelibrary.wiley.com/doi/10.1002/9781444304992.ch7/summary [Accessed: 15 July 2017].

Law, J. and Callon, M. (1988). Engineering and Sociology in a Military Aircraft Project: A Network Analysis of Technological Change. *Social Problems*35:284–297.

Law, J. and Urry, J. (2004). Enacting the social. *Economy and Society*33:390–410.

Law, J. and Singleton, V. (2013). ANT and Politics: Working in and on the World. *Qualitative Sociology*36:485–502.

Leavy, P. (2014). *The Oxford Handbook of Qualitative Research*. Oxford University Press.

Leckner, S. (2018). Sceptics and supporters of corporate use of behavioural data: Attitudes towards informational privacy and Internet surveillance in Sweden. *Northern Lights.*16(1):113-132.

Lee, I. (2016). *Encyclopedia of E-Commerce Development, Implementation, and Management*. IGI Global.

Lee, J.G. and Scott, G.G. (2017). *Preventing Credit Card Fraud: A Complete Guide for Everyone from Merchants to Consumers*. Rowman & Littlefield.

Lepoivre, M.R., Avanzini, C.O., Bignon, G., Legendre, L. and Piwele, A.K. (2016). Credit Card Fraud Detection with Unsupervised Algorithms. *Journal of Advances in Information Technology*7:34–38.

Leukfeldt, E.R. (2017). *Research Agenda The Human Factor in Cybercrime and Cybersecurity* [online]. Available at: https://www.thehaguesecuritydelta.com/media/com_hsd/report/141/document/Research-Agenda-The-Human-Factor-in-Cybercrime-and-Cybersecurity.pdf [Accessed: 21 May 2018].

Leukfeldt, E.R. (ed.) (2017). *The Human Factor in Cybercrime and Cybersecurity: Research Agenda*. The Netherlands: Eleven International Publishing.

Leukfeldt, E. R. and Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*. 37 (3), 263–280.

Leukfeldt, E.R., Lavorgna, A. and Kleemans, E.R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*23:287–300.

Leung, V.C., Lai, R.X., Chen, M. and Wan, J. (2015). *Cloud Computing: 5th International Conference, CloudComp 2014, Guilin, China, October 19-21, 2014, Revised Selected Papers*. Springer.

Leurs, K. and Shepherd, T. (2017). Datafication and Discrimination. In: Schaefer, M and van Es, K. (ed.) *The Datafied Society: Studying Culture Through Data*. Amsterdam University Press.

Levi, M., Burrows, J., Fleming, M., Hopkins, M. and Matthews, K.G.P. (2007). The nature, extent and economic impact of fraud in the UK.

Levi, M., Doig, A., Gundur, R.V., Wall, D. and Williams, M. (2015). *The Implications of Economic Cybercrime for Policing*. City of London Corporation.

Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law and Social Change*67:77–96.

Lewig, K. A. and Dollard, M. F. (2003). Emotional dissonance, emotional exhaustion and job satisfaction in call centre workers. *European Journal of Work and Organizational Psychology*. 12 (4), 366–392.

Leyed, J. (2014). *The Guide to E-Commerce Fraud* [online]. Available at: https://www.2checkout.com/upload/documents/ebook_Guide_to_Ecommerce_Fra

ud.pdf [Accessed: 12 May 2018].

Li, J., Cao, L., Wang, C., Tan, K.C., Liu, B., Pei, J. and Tseng, V.S. (2013). *Trends and Applications in Knowledge Discovery and Data Mining: PAKDD 2013 Workshops: DMApps, DANTH, QIMIE, BDM, CDA, CloudSD, Golden Coast, QLD, Australia, Revised Selected Papers*. Springer.

Lichtman, M. (2013). *Qualitative Research for the Social Sciences*. SAGE Publications.

Linxweiler, J.A. (2016). *Botnets. Economics of Cybercrime*. GRIN Verlag.

Lippens, R. and Calster, P.V. (2010). *New Directions for Criminology: Notes from Outside the Field*. Maklu.

Lloyd, D. A. (2013). *Labour Markets and Identity on the Post-Industrial Assembly Line*. Ashgate Publishing, Ltd.

Loader, B.D. (ed.) (2000). *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Routledge.

Lovett, F. (2006). Rational Choice Theory and Explanation. *Rationality and Society*. 18 (2), 237–272.

Lourenco, R. (2018). *Three e-commerce fraud challenges to beat in 2018* [online]. Available at: https://www.digitalcommerce360.com/2018/02/08/three-e-commerce-fraud-challenges-beat-2018/ [Accessed: 12 May 2018].

Lowe, P., Boden, S., Williams, S.J., Seale, C. and Steinberg, D.L. (2008). *The Social Construction of Sleep and Work in the British Print News Media* [online]. Available at: https://research.aston.ac.uk/portal/en/researchoutput/the-social-construction-of-sleep-and-work-in-the-british-print-news-media(5869c79e-3d59-4838-89c8-009a5ea33bf1).html [Accessed: 21 December 2016].

Lowry, D. (2004). Understanding Reproductive Technologies as a Surveillant Assemblage: Revisions of Power and Technoscience. *Sociological Perspectives,47*(4), 357-370.

Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal, Canadian Edition*7:35–49.
Lupton, D. (2014). *Digital Sociology*. Routledge.

Lusthaus, J. and Varese, F. (2017). *Offline and Local: The Hidden Face of Cybercrime* [online]. Available at: https://academic.oup.com/policing/advance-article/doi/10.1093/police/pax042/4055914 [Accessed: 21 May 2018].

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. McGraw-Hill Education (UK).

Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Psychology Press.

Lyon, D. (2004). Identity Cards: Social Sorting by Database. *SSRN Electronic Journal* [online]. Available from: http://www.ssrn.com/abstract=1325259 (Accessed 24 February 2019).

Lyon, D. (2006). *Theorizing Surveillance*. Routledge.

Lyon, D. (2007a). Surveillance, Security and Social Sorting: Emerging Research Priorities. *International Criminal Justice Review* [online] 17 (3), 161–170.

Lyon, D. (2007b). *Surveillance Studies: An Overview*. Polity.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society* [online] 1 (2).

Lytras, M.D., Ruan, D., Tennyson, R.D., Pablos, P.O.D., Peñalvo, F.J.G. and Rusu, L. (2013). *Information Systems, E-Learning, and Knowledge Management Research: 4th World Summit on the Knowledge Society, WSKS 2011, Mykonos, Greece, September 21-23, 2011. Revised Selected Papers*. Springer.

Macdonald, C. and Best, S. (2016). *Dubai Police Launch AI That Can Spot Crimes BEFORE They Happen* [online]. Available at: http://www.dailymail.co.uk/~/article-4062936/index.html [Accessed: 16 January 2018].

MacKenzie, D.A. (1993). *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*. MIT Press.

Magnusson, E. and Marecek, J. (2015). *Doing Interview-Based Qualitative Research: A Learner's Guide*. Cambridge University Press.

Maguire, M., Morgan, R. and Reiner, R. (eds.) (2007). *The Oxford Handbook of Criminology*. 4th edition. OUP Oxford.

Makhabel, B. (2015). *Learning Data Mining with R*. Packt Publishing Ltd.

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security* [online] 2013 (6), 9–13.

Marcum, C.D. (2015). *Cyber Crime*. Wolters Kluwer Law & Business.

Marlow, A. (2014). Thinking about the fall in crime. *Safer Communities* [online].

Available at: http://www.emeraldinsight.com/doi/abs/10.1108/SC-01-2014-0001 [Accessed: 25 January 2018].

Marr, B. (2016). *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results*. John Wiley & Sons.

Marsh, I. (2002). *Theory and Practice in Sociology*. Pearson Education.

Marshall, C. and Rossman, G.B. (2014). *Designing Qualitative Research*. SAGE Publications.

Martellozzo, E. and Jane, E.A. (2017). *Cybercrime and Its Victims*. Taylor & Francis.

Marvasti, A. (2004). *Qualitative Research in Sociology*. SAGE Publications.

Marvin, R. (2016). *Predictive Analytics, Big Data, and How to Make Them Work for You* [online]. Available at: http://uk.pcmag.com/salesforcecom-professional-edition/82910/feature/predictive-analytics-big-data-and-how-to-make-them-work-for [Accessed: 13 April 2017].

Masys, A.J. (2014). *Networks and Network Analysis for Defence and Security*. Springer Science & Business Media.

Matthews, M.R. (2012). *Constructivism in Science Education: A Philosophical Examination*. Springer Science & Business Media.

Matzner, T. (2016). Beyond data as representation: The performativity of Big Data in surveillance. *Surveillance & Society*. 14 (2), 197–210.

Mawby, R. and Gill, M. (2017). Critiquing the regulation of private security in the United Kingdom: views from inside the sector. *International Journal of Comparative and Applied Criminal Justice*. 1–14.

Mayer-Schönberger, V. and Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.

McGuire, M., Dowling, S. (2013*). Cyber crime: A review of the evidence. Research Report 75. Summary of key findings and implications* [online]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf [Accessed: 23 September 2018].

McIlveen, P. (2008). Autoethnography as a method for reflexive research and practice in vocational psychology. *Australian Journal of Career Development*. 17(2), 13-20.

McLaughlin, E. and Newburn, T. (2010). *The SAGE Handbook of Criminological*

Theory. SAGE.

Mena, J. (2003). *Investigative Data Mining for Security and Criminal Detection*. Butterworth-Heinemann.

Meng, Y. (2014). Racially biased policing and neighborhood characteristics: A Case Study in Toronto, Canada. *Cybergeo: European Journal of Geography*.

Merriam, S.B. and Tisdell, E.J. (2015). *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons.

Metcalf, J. and Crawford, K. (2016). Where are human subjects in Big Data research? The emerging ethics divide. *Big Data & Society*3:2053951716650211.

Michael, M. (2012). *Reconnecting Culture, Technology and Nature: From Society to Heterogeneity*. Routledge.

Michael, M. (2016). *Actor-Network Theory: Trials, Trails and Translations*. SAGE.

Miettinen, R. (1999). The riddle of things: Activity theory and actor-network theory as approaches to studying innovations. *Mind, Culture, and Activity*6:170–195.

Miller, J. (2009). *21st Century Criminology: A Reference Handbook*.

Minelli, M., Chambers, M. and Dhiraj, A. (2012). *Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses*. John Wiley & Sons.

Ministry of Justice (2017). *FOI releases for April 2017. Computer Misuse Act 1990 convictions tables* [online]. Available from: https://www.gov.uk/government/publications/foi-releases-for-april-2017 (Accessed 17 February 2019).

Mlambo, G. (2013). *Affiliate Mind: Internet Riches*. Booktango.

Mol, A. (1999). Ontological Politics. A Word and Some Questions. *The Sociological Review.*47:74–89.

Montague, D.A. (2010). *Essentials of Online Payment Security and Fraud Prevention*. John Wiley & Sons.

Moore, R. (2014). *Cybercrime: Investigating High-Technology Computer Crime*. Routledge.

Moore, M. and Morris, M. B. (2011). Political Science Theories of Crime and Delinquency. *Journal of Human Behavior in the Social Environment*. 21 (3), 284–296.

Moore, R. T. and Reeves, A. (2016). *Defining Racial and Ethnic Context with*

Geolocation Data. 28 [online]. Available at: https://pdfs.semanticscholar.org/7451/e0374b28d7fe480297b76f5c92012dbc0a69.pdf

Morgan, S. (2017). *2017 Cybercrime Report. Cybercrime damages will cost the world $6 trillion annually by 2021* [online]. Available at: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf [Accessed: 12 May 2018].

MRC Blog (2018). *Circumventing Fraud Trends in 2018* [online]. Available at: http://www.merchantriskcouncil.org/news-and-press/mrc-blog/2018/circumventing-fraud-trends-in-2018 [Accessed: 12 May 2018].

MRC Blog (2018). *The Seven Types of ECommerce Fraud* [online]. Available at: http://www.merchantriskcouncil.org/news-and-press/mrc-blog/2018/the-seven-types-of-ecommerce-fraud [Accessed: 12 May 2018].

Müller, M. (2015). Assemblages and Actor-networks: Rethinking Socio-material Power, Politics and Space. *Geography Compass*9:27–41.

Muncie, J. and McLaughlin, E. (2001). *The Problem of Crime*. SAGE.

Mützel, S. (2015). Facing Big Data: Making sociology relevant. *Big Data & Society*2:2053951715599179.

Mythen, G. (2014). *Understanding the Risk Society: Crime, Security and Justice*. Palgrave Macmillan.

Natifu, B. (2016). *Multiple levels of "knowing and being known", their affiliated capital, benefits and challenges.* [online]. Available at: https://www.growkudos.com/publications/10.1108%252Fjoe-09-2015-0022 [Accessed: 25 January 2018].

National Audit Office (2017). *Online Fraud* [online]. Available from: https://www.nao.org.uk/report/online-fraud/ (Accessed 17 February 2019).

Neef, D. (2014). *Digital Exhaust: What Everyone Should Know About Big Data, Digitization and Digitally Driven Innovation*. Pearson Education.

Nelson, P. (2018). *Betrugserkennung über Big Data – Fallbeispiel aus der Versicherungsbranche* [Online]. Available at: https://www.searchtechnologies.com/de/blog/big-data-betrugserkennung [Accessed: 16 January 2018].

Nettleton, D. (2014). *Commercial Data Mining: Processing, Analysis and Modeling*

for Predictive Analytics Projects. Elsevier.

Neustaedter, C. and Smith, M. A. (2004). '*Beyond "From" and "Received": Social Sorting for Email Triage*'.

Newburn, T. (2008). *Handbook of Policing*. Routledge.

Newton, T., Deetz, S. and Reed, M. (2011). Responses to Social Constructionism and Critical Realism in Organization Studies. *Organization Studies*, 32(1), pp.7–26.

Neyland, D. (2006). Dismissed Content and Discontent: An Analysis of the Strategic Aspects of Actor-Network Theory. *Science, Technology, & Human Values.* 31:29–51.

Neyland, D. and Möllers, N. (2016). Algorithmic IF … THEN rules and the conditions and consequences of power. *Information, Communication & Society*:1–18.

Ngo, F. T. and Paternoster, R. (2011). *Cybercrime Victimization: An examination of Individual and Situational level factors*. International Journal of Cyber Criminology. 5 (1), 21.

Nimmo, R. (2011). *Actor-Network Theory and Methodology: Social Research in a More-Than-Human World* [online]. Available at: https://www.escholar.manchester.ac.uk/uk-ac-man-scw:134378 [Accessed: 7 January 2018].

Nisbet, R., Elder, J. and Miner, G. (2009). *Handbook of Statistical Analysis and Data Mining Applications*. Academic Press.

Nord, W. R. and Connell, A. F. (2012). *Rethinking the Knowledge Controversy in Organization Studies: A Generative Uncertainty Perspective*. Routledge.

Nunes, J.A. (2012). Review of *The Problem of Relativism in the Sociology of (Scientific) Knowledge* [online]. Available at: http://ndpr.nd.edu/news/34559-the-problem-of-relativism-in-the-sociology-of-scientific-knowledge/ [Accessed: 21 December 2016].

O'Brien, M. and Yar, M. (2008). *Criminology: The Key Concepts*. Routledge.

Office for National Statistics (2018).*Crime in England and Wales* [online]. Available from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016 (Accessed 17 February 2019).

Olayemi, O.J. (2014). *A socio-technological analysis of cybercrime and cyber security in Nigeria*. International Journal of Sociology and Anthropology. 6(3): 116-125.

Olshannikova, E., Olsson, T., Huhtamäki, J. and Kärkkäinen, H. (2017). Conceptualizing Big Social Data. *Journal of Big Data*4:3.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown.

Ong, P.M. and Stoll, M. (2008). Why Do Inner City Residents Pay Higher Premiums? The Determinants of Automobile Insurance Premiums. *University of California Transportation Center, University of California Transportation Center, Working Papers*, 1 January 2008.

O'Shea, J. (2017). Contactless payment fraud soars. *BBC News* [online]. Available at: http://www.bbc.com/news/uk-england-devon-39942246 [Accessed: 25 January 2018].

O'Sullivan, T. (2010). *Decision Making in Social Work*. Palgrave Macmillan.

Owen, T., Noble, W. and Speed, F.C. (2017). *New Perspectives on Cybercrime*. Springer.

Oxford Dictionaries (n.d.). *Cybercrime | Definition of cybercrime in English by Oxford Dictionaries* [online]. Available from: https://en.oxforddictionaries.com/definition/cybercrime (Accessed 8 March 2019).

Paetz, P. (2014). *Disruption by Design: How to Create Products That Disrupt and Then Dominate Markets*. Apress.

Parikh (2010). *Organisational Behaviour*. Tata McGraw-Hill Education.

Parker, I. (1998). *Social Constructionism, Discourse and Realism*. SAGE.

Parra-Arnau, J. and Castelluccia, C. (2018). *Dataveillance and the False-Positive Paradox*. HAL. 11.

Pascual, A., Marchini, K., Sposito, S. (2018). *Fraud & Security Trends* [online]. Available at: https://www.javelinstrategy.com/coverage-area/2018-fraud-security-trends [Accessed: 12 May 2018].

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

Payton, T. and Claypoole, T. (2014). *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. Rowman & Littlefield.

Peachey, K. (2016). *Financial scams seen 'every 15 seconds'* [online]. Available from: https://www.bbc.com/news/business-37411036 (Accessed 17 February 2019).

Peelo, M. and Soothill, K. (2013). *Questioning Crime and Criminology*. Routledge.

Perry, W.L. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. CA: RAND.

Perry, W.L., McInnis, B., Price, C.C., Smith, S. and Hollywood, J.S. (2013). *Predictive Policing* [online]. Available at: https://www.rand.org/pubs/research_reports/RR233.html [Accessed: 14 July 2017].

Phillips, J. (2013). *Digital Analytics Primer*. FT Press.

Pinch, T.J. and Bijker, W.E. (1984). The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science*, 14(3), pp.399–441.

Pitts, V. (2017). *Cyber Crimes: History of World's Worst Cyber Attacks*. Vij Books India Pvt Ltd.

Piquero, A. R. and Tibbets, S. G. (2001). *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*. Routledge.

Polizzi, D. (2015). *A Philosophy of the Social Construction of Crime*. Policy Press.

Polman, T. and Spruit, M. (2011). Integrating Knowledge Engineering and Data Mining in e-commerce Fraud Prediction. In: *Information Systems, E-Learning, and Knowledge Management Research*. Springer, Berlin, Heidelberg, pp. 460–466. Available at: https://link.springer.com/chapter/10.1007/978-3-642-35879-1_56 [Accessed: 17 April 2017].

Potter, J. (1996). *Representing Reality: Discourse, Rhetoric and Social Construction*. SAGE.

Press, O.U. (2010). *The Social Construction of Crime: Oxford Bibliographies Online Research Guide*. Oxford University Press, USA.

Provost, F. and Fawcett, T. (2013a). Data Science and its Relationship to Big Data and Data-Driven Decision Making. *Big Data*1:51–59.

Provost, F. and Fawcett, T. (2013b). *Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking*. O'Reilly Media, Inc.

Purtill, C. (2015). *The US is using a race-predicting algorithm to identify victims of car loan discrimination* [online]. Available at: https://qz.com/537816/in-an-auto-loan-discrimination-case-a-race-predicting-algorithm-is-the-us-governments-best-shot-at-paying-victims-back/ [Accessed: 25 January 2018].

Quinney, R. (1970). *The Social Reality of Crime*. Transaction Publishers.

Rafter, N.H. and Brown, M. (2011). *Criminology Goes to the Movies: Crime Theory and Popular Culture*. NYU Press.

Reiman, J.H. and Leighton, P. (2013). *The Rich Get Richer and the Poor Get Prison: Ideology, Class, and Criminal Justice*. 10th ed. Boston: Pearson.

Reiner, R. (2016). *Crime, the Mystery of the Common-Sense Concept*. Malden, MA: Polity Press.

Restivo, S. and Croissant, J. (2018). *Social constructionism in science and technology studies.* Available at: https://www.academia.edu/594563/Social_constructionism_in_science_and_technology_studies [Accessed: 21 December 2016].

Reviews, C.T.I. (2016). *Essentials of Business Research, A Guide to Doing Your Research Project: Business, Business*. Cram101 Textbook Reviews.

Richards, N.M. and King, J.H. (2014). *Big Data Ethics*. Rochester, NY: Social Science Research Network. Available at: https://papers.ssrn.com/abstract=2384174 [Accessed: 13 June 2017].

Rigby, M. and Sanchis, E. (2006). *The Concept of Skill and Its Social Construction*.

Riskified (2017). *Fighting CNP Fraud in Fashion. A Special report for retailers* [online]. Available at: https://blog.riskified.com/our-2017-report-on-fighting-fraud-in-online-fashion/ [Accessed: 12 May 2018].

Robert, D. and Dufresne, M. (2016). *Actor-Network Theory and Crime Studies: Explorations in Science and Technology*. Routledge.

Roberts, J.M. (2012). Poststructuralism against poststructuralism: Actor-network theory, organizations and economic markets. *European Journal of Social Theory*15:35–53.

Robinson, D. and Yu, H. (2014). *Civil Rights, Big Data, and Our Algorithmic Future* [online]. Available at: https://bigdata.fairness.io/ [Accessed: 16 January 2018].

Robles, J.S. (2012). *A Discourse Analysis of "Social Construction" in Communication Scholarship* [online]. Available at: http://www.cios.org/EJCPUBLIC/022/3/022342.html [Accessed: 21 December 2016].

Rosenfeld, R. (2010). *The Social Construction of Crime: Oxford Bibliographies Online Research Guide*. Oxford University Press, USA.

Ross, L.E. (2017). An account from the inside: Examining the emotional impact of qualitative research through the lens of 'insider' research. *Qualitative Psychology (Washington, D.C.)*4:326–337.

Ruckenstein, M. (2014). Visualized and Interacted Life: Personal Analytics and Engagements with Data Doubles. *Societies*. 4 (1), 68–84.

Ruppert, E. (2013). Rethinking empirical social sciences. *Dialogues in Human Geography*3:268–273.

Ruppert, E., Law, J. and Savage, M. (2013). Reassembling Social Science Methods: The Challenge of Digital Devices. *Theory, Culture & Society*30:22–46.

Russell, B. (2009). *Smiling Down the Line: Info-service Work in the Global Economy*. University of Toronto Press.

Rydin, Y. and Tate, L. (2016). *Actor Networks of Planning: Exploring the Influence of Actor Network Theory*. Routledge.

Saldana, J. (2015). *The Coding Manual for Qualitative Researchers*. SAGE.

Saldanha, A. (2003). Review Essay: Actor-Network Theory and Critical Sociology. *Critical Sociology*29:419–432.

Samet, O. (2013). *Introduction to Online Payments Risk Management*. O'Reilly Media, Inc.

Sammons, J. and Cross, M. (2016). *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy*. Elsevier.

Samonas, S. (2013). *Insider fraud and routine activity theory* [online]. Available from: http://www.security-conference.org/index.php/secconf/secconf12 (Accessed 1 March 2019).

Sandoval, M. (2014). *From Corporate to Social Media: Critical Perspectives on Corporate Social Responsibility in Media and Communication Industries*. Routledge.

Saraga, E. (2005). *Embodying the Social: Constructions of Difference*. Routledge.

Satell, G. (2014). *5 Things Managers Should Know About The Big Data Economy* [online]. Available at: http://www.forbes.com/sites/gregsatell/2014/01/26/5-things-managers-should-know-about-the-big-data-economy/ [Accessed: 7 March 2017].

Sathi, A. (2014). *Engaging Customers Using Big Data: How Marketing Analytics Are Transforming Business*. Palgrave Macmillan.

Savage, M. (2012). *The PayPal Official Insider Guide to Internet Security: Spot Scams and Protect Your Online Business*. Peachpit Press.

Schäfer, M. T. and Es, K. van (2017). *The datafied society: studying culture through data*. Amsterdam University Press.

Schatzki, T.R., Knorr-Cetina, K. and Savigny, E. von (eds.) (2001). *The Practice Turn in Contemporary Theory*. New York: Routledge.

Scheer, R. (2015). *They Know Everything About You: How Data-Collecting Corporations and Snooping Government Agencies Are Destroying Democracy*. Nation Books.

Schell, B. H. and Martin, C. (2004). *Cybercrime: A Reference Handbook*. ABC-CLIO.

Schmidgen, H. (2014). *Bruno Latour in Pieces: An Intellectual Biography*. Fordham University Press.

Schroeder, R. (2014). Big Data and the brave new world of social media research. *Big Data & Society*1:2053951714563194.

Schroeder, R. and Cowls, J. (2014). Big data, ethics, and the social implications of knowledge production. In: *Data Ethics Workshop, KDD@ Bloomberg, August*.

Schuchter, A. and Levi, M. (2016). The Fraud Triangle revisited. *Security Journal*29:107–121.

Schweidel, D.A. (2014). *Profiting from the Data Economy: Understanding the Roles of Consumers, Innovators and Regulators in a Data-Driven World*. Pearson Education.

Searle, J.R. (1995). *The Construction of Social Reality*. Simon and Schuster.

Seely, B. (2016). *Cyber Fraud: The Web of Lies: US Marine Risks Life in Prison to Expose a Cybercrime That Consumers Know Nothing About*. CreateSpace Independent Publishing Platform.

Seidman, I. (2015). *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences, 4th Ed.* Teachers College Press.

Sensing, T. (2011). *Qualitative Research: A Multi-Methods Approach to Projects for Doctor of Ministry Theses*. Wipf and Stock Publishers.

Shalal, A. (2017). Germany sees rise in cybercrime, but reporting rates still low. *Reuters*. Available from: https://www.reuters.com/article/us-germany-cybercrime-crime-idUSKBN17Z26S (Accessed 17 February 2019).

Shapira, Z. (2002). *Organizational Decision Making*. Cambridge University Press.

Shapiro, A. (2018). Street-level: Google Street View's abstraction by datafication. *New Media & Society*. 20 (3), 1201–1219.

Sharp, D. (2003). *Call Center Operation: Design, Operation, and Maintenance*. Digital Press.

Shavers, B. (2012). *Cybercrime Investigation Case Studies: An Excerpt from Placing the Suspect Behind the Keyboard*. Newnes.

Shaw, R. (2015). Big Data and reality. *Big Data & Society*2:2053951715608877.

Shire, K. A. et al. (2017). *Re-organising Service Work: Call Centres in Germany and Britain: Call Centres in Germany and Britain*. Routledge.

Siciliano, R. (2011). *99 Things You Wish You Knew Before-- Your Identity Was Stolen: Your Guide to Protecting Yourself from Identity Theft and Computer Fraud*. Ginger Marks.

Siegel, E. (2016). *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*. John Wiley & Sons.

Sikes, P. and Potts, A. (2008). *Researching Education from the Inside: Investigations from Within*. Routledge.

Silverman, D. (2013). *Doing Qualitative Research: A Practical Handbook*. SAGE.

Silverman, D. (2015). *Interpreting Qualitative Data*. SAGE.

Silverman, D. (2017). *Doing Qualitative Research*. SAGE.

Singh, D.J. and Davidson, J. (2015). *Introduction to Internet Scams and Fraud - Credit Card Theft, Work-At-Home Scams and Lottery Scams*. Mendon Cottage Books.

Sismondo, S. (2011). *An Introduction to Science and Technology Studies*. John Wiley & Sons.

Smith, R.G., Grabosky, P. and Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge University Press.

Smith, V. (2013). *Sociology of Work: An Encyclopedia*. SAGE Publications.

Space, S.S. (2016). *Who Is Doing Big Data: A SAGE Survey* [online]. Available at: http://www.socialsciencespace.com/2016/09/big-data-sage-survey/ [Accessed: 8 March 2017].

Spetalnick, M. and Brunnstrom, D. (2015). *China in focus as cyber attack hits millions of U.S. federal workers* [online]. Available at: https://www.reuters.com/article/us-cybersecurity-usa/massive-cyber-attack-hits-u-s-federal-workers-probe-focuses-on-china-idUSKBN0OK2IK20150605 [Accessed: 16 January 2018].

Spickard, J.V. (2016). *Research Basics: Design to Data Analysis in Six Steps*. SAGE Publications.

Spoof Card (n.d.). *Spoof Calls & Change Your Caller ID* [online]. Available from: https://www.spoofcard.com/secondary-callerid (Accessed 24 February 2019).

Sridhar, R. (2017). *How Is Data Analytics Shaping the Future of E-Commerce?* [online]. Available at: http://blog.csscorp.com/analytics/data-analytics-shaping-future-e-commerce [Accessed: 18 April 2017].

Stam, H.J. (2001). *Introduction: Social Constructionism and Its Critics*. Sage Publications Sage CA: Thousand Oaks, CA.

Stamler, R.T., Marschdorf, H.J. and Possamai, M. (2014). *Fraud Prevention and Detection: Warning Signs and the Red Flag System*. CRC Press.

Steinmetz, K.F. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime*. NYU Press.

Stoddart, E. (2014). (In)visibility Before Privacy: A Theological Ethics of Surveillance as Social Sorting. *Studies in Christian Ethics*. 27 (1), 33–49.

Stratton, G., Powell, A. and Cameron, R. (2017). *Crime and Justice in Digital Society: Towards a 'Digital Criminology'?* [online]. *International Journal for Crime, Justice and Social Democracy* [online]. Available from: https://www.crimejusticejournal.com/article/view [accessed 1 March 2019].

Storr, V.H. (2010). The Social Construction of the Market. *Society*47:200–206.

Strong, C. (2015). *Humanizing Big Data: Marketing at the Meeting of Data, Social Science and Consumer Insight*. Kogan Page Publishers.

Subramanian, R. (2014). *Bank Fraud: Using Technology to Combat Losses*. John Wiley & Sons.

Sumathi, S. and Sivanandam, S.N. (2006). *Introduction to Data Mining and Its Applications*. Springer.

Sveinsdóttir, Á. (2015). Social Construction. *Philosophy Compass*10:884–892.

Sweeney, L. (2013). *Discrimination in Online Ad Delivery*. Social Science Research Network. Available at: https://papers.ssrn.com/abstract=2208240 [Accessed: 16 January 2018].

Syal, R. and Haddou, L. (2014). *Passport Office targeting 100 postcodes for fraud investigations* [online]. Available at: https://www.theguardian.com/politics/2014/sep/09/passport-office-targeting-100-postcodes-fraud-investigations [Accessed: 7 July 2017].

Symantec (2015). *Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust* [online]. Available at: https://www.symantec.com/content/dam/symantec/docs/white-papers/cybersecurity-retail-en.pdf [Accessed: 11 May 2018].

Symantec Corporation (2018).*2017 Norton Cyber Security Insights Report - Global Results*. 30.

Symantec Corporation (n.d.). *Norton Cybercrime Report: The Human Impact* [online]. Available from: https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf (Accessed 9 March 2019).

Symons, J. and Alvarado, R. (2016). Can we trust Big Data? Applying philosophy of science to software. *Big Data & Society*3:2053951716664747.

Tabak, E. (2015). *Information Cosmopolitics: An Actor-Network Theory Approach to Information Practices*. Chandos Publishing.

Tanner, R.E.S. (2008). *Contemporary Social Science Research*. Concept Publishing Company.

Tänzler, D. and Maras, K. (2016). *The Social Construction of Corruption in Europe*. Routledge.

Tatnall, A. (2001). *Social and Professional Applications of Actor-Network Theory for Technology Development*. IGI Global. Available at: http://www.igi-global.com/book/social-professional-applications-actor-network/67406 [Accessed: 21 December 2016].

Tayebi, M.A. and Glässer, U. (2016). *Social Network Analysis in Predictive Policing: Concepts, Models and Methods*. Springer.

Teusner, A. (2015). Insider research, validity issues, and the OHS professional: one person's journey. *International Journal of Social Research Methodology* [online]. Available at: http://www-tandfonline-com.libprox.gold.ac.uk:2048/doi/abs/10.1080/13645579.2015.1019263 [Accessed: 25 January 2018].

The Crown Prosecution Service (n.d.). *Cybercrime - prosecution guidance* [online]. Available from: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (Accessed 17 February 2019).

Thibodeaux, J. (2014). Three Versions of Constructionism and their Reliance on Social Conditions in Social Problems Research. *ResearchGate*48:829–837.

ThreatMetrix (2013). *Five Trends to Track in E-Commerce Fraud* [online]. Available at: http://info.threatmetrix.com/rs/threatmetrix/images/Five_Trends_eCommerce_Fraud_WP.pdf [Accessed: 12 May 2018].

ThreatMetrix (2018).*Q1 2018 Cybercrime Report* [online]. Available from: https://www.threatmetrix.com/info/q1-2018-cybercrime-report/ (Accessed 17 February 2019).

Tilley, N. and Sidebottom, A. (2017). *Handbook of Crime Prevention and Community Safety*. Routledge.

Tkatchuk, R. (2017). *5 Ecommerce Fraud Predictions for 2017* [online]. Available at: http://www.networkworld.com/article/3173322/security/5-ecommerce-fraud-predictions-for-2017.html [Accessed: 17 April 2017].

Tonelli, D., Soares Da Silva, S. and Zambalde, A. (2018). *The Critical Constructivism of the Actor-Network Theory and the Knowledge-Based Economy of the Triple Helix: Theoretical Possibilities and Practical Implications 1*.

Tracy, R.M. (2005). *Reduce Your Risk of Credit Fraud and Identity Theft!* The Privacy Trust Group.

Treadwell, J. (2012). *Criminology: The Essentials*. SAGE.

Tsoukas, H. (2000). False Dilemmas in Organization Theory: Realism or Social Constructivism? *Organization*7:531–535.

Turner, B.S. (2009). *The New Blackwell Companion to Social Theory*. John Wiley & Sons.

Ugwudike, P. (2015). *An Introduction to Critical Criminology*. Policy Press.

UK Finance (2018). *Fraud the Facts 2018. The definitive overview of payment industry fraud* [online]. Available at: https://www.ukfinance.org.uk/wp-content/uploads/2018/07/Fraud-the-facts-Digital-version-August-2018.pdf [Accessed: 12 May 2018].

UK Fraud Costs Measurement Committee (UKFCMC) (2017). *Annual Fraud Indicator 2017* [online]. Available from: https://brand.crowe.co.uk/wp-content/uploads/sites/2/2017/11/Annual-fraud-indicator-2017.pdf (Accessed 9 March 2019).

Van der Schyff, K., Krauss, K. and Kroeze, J. (2018). Facebook and Dataveillance: Demonstrating a Multimodal Discourse Analysis. *AMCIS 2018 Proceedings* [online]. Available from: https://aisel.aisnet.org/amcis2018/Philosophy/Presentations/1. (Accessed 1 March 2019).

Van Heugten, K. (2004). Managing Insider Research: Learning from Experience. *Qualitative Social Work*. 3 (2), 203–219.

Venters, W. (2010). Knowledge management technology-in-practice: a social constructionist analysis of the introduction and use of knowledge management systems. *Knowledge Management Research & Practice*8:161–172.

Venturini, T. (2009). Diving in magma: how to explore controversies with actor-network theory. *Public Understanding of Science* [online]. Available at: http://journals.sagepub.com/doi/10.1177/0963662509102694 [Accessed: 25 January 2018].

Viano, E.C. (2016). *Cybercrime, Organized Crime, and Societal Responses: International Approaches*. Springer.

Villing, L. and Bohland, N. (2016). *Industrie 4.0 und Cybercrime. Sicherheitskonzepte für Cybersecurity*. GRIN Verlag.

Visser, M. (2010). Constructing organisational learning and knowledge socially: an interactional perspective. *International Journal of Knowledge and Learning*6:285–294.

Volti, R. (2011). *An Introduction to the Sociology of Work and Occupations*. Pine Forge Press.

Vona, L.W. (2011). *The Fraud Audit: Responding to the Risk of Fraud in Core Business Systems*. John Wiley & Sons.

Vona, L.W. (2017). *Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems*. John Wiley & Sons.

Vona, L.W. (2012). *Fraud Risk Assessment: Building a Fraud Audit Program*. John Wiley & Sons.

Vuitton, E. (2017). *Ecommerce Payment Fraud Outlook 2017-2020* [online]. Available at: https://chargeback.com/ecommerce-payment-fraud-outlook-2020/ [Accessed: 12 May 2018].

Waddell, K. (2016). *How Algorithms Can Bring Down Minorities' Credit Scores* [online]. Available at: https://www.theatlantic.com/technology/archive/2016/12/how-algorithms-can-bring-down-minorities-credit-scores/509333/ [Accessed: 25 January 2018].

Wagen, W. van der and Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *British Journal of Criminology*55:578–595.

Wagner-Pacifici, R., Mohr, J.W. and Breiger, R.L. (2015). Ontologies, methodologies, and new uses of Big Data in the social and cultural sciences. *Big Data & Society*2:2053951715613810.

Walker, Z. (2015). *'Ship To' Address Changes: A Growing Concern For e-Commerce Fraud* [online]. Available at: http://info.rippleshot.com/blog/ship-to-address-growing-concern-for-ecommerce-fraud [Accessed: 18 April 2017].

Walklate, S. (2007). *Understanding Criminology: Current Theoretical Debates*. McGraw-Hill Education (UK).

Wall, D.S. (ed.) (2001). *Crime and the Internet: Cybercrimes and Cyber fears*. New York: Routledge.

Wall, D.S. (2004). Digital Realism and the Governance of Spam as Cybercrime. *European Journal on Criminal Policy and Research*10:309–335.

Wall, D.S. (2005). The Internet as a Conduit for Criminal Activity. In: *Information Technology and the Criminal Justice System*. SAGE Publications, Inc., pp. 77–98. Available at: http://sk.sagepub.com/books/information-technology-and-the-criminal-justice-system/n4.xml [Accessed: 19 September 2018].

Wall, S. (2006). An Autoethnography on Learning about Autoethnography. *International Journal of Qualitative Methods*. 5(2).

Wall, D.S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

Wall, D.S. (2007/10). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (Revised May 2010*), Police Practice & Research: An International Journal*, 8(2):183 205.

Wall, D.S. (2011). *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace* [online]. Available at: http://www.cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf [Accessed: 12 May 2018].

Wall, D.S. (2015). *The Internet as a Conduit for Criminal Activity*. Social Science Research Network. Available at: https://papers.ssrn.com/abstract=740626 [Accessed: 25 January 2018].

Wall, D.S. (2017). *Cyberspace Crime*. Routledge.

Wall, D.S. and Williams, M. (2017). *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*. Routledge.

Wang, X., Gerber, M.S. and Brown, D.E. (2012). Automatic Crime Prediction Using Events Extracted from Twitter Posts. In: *Social Computing, Behavioral - Cultural Modeling and Prediction*. Springer, pp. 231–238. Available at: https://link.springer.com/chapter/10.1007/978-3-642-29047-3_28 [Accessed: 16 March 2017].

Wang, X., White, L. and Chen, X. (2015). *Big data research for the knowledge economy: past, present, and future* [online]. Available at: http://www.emeraldinsight.com/doi/full/10.1108/IMDS-09-2015-0388 [Accessed: 6 March 2017].

Ward, T. (2010). Strategies for Reducing the Risk of eCommerce Fraud. *Atlanta: First Data Corporation*.

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime*. Apress.

Watson, T. (2004). *Sociology, Work and Industry: Fifth edition*. Routledge.

Watson, T. (2017). *Sociology, Work and Organisation: Seventh Edition*. Taylor & Francis.

Webster, W. and Ball, K. (2018). *Surveillance and Democracy in Europe: Courting Controversy?* Routledge.

Wells, J.T. (2010). *Internet Fraud Casebook: The World Wide Web of Deceit*. John Wiley & Sons.

Whitty, M.T. and Joinson, A. (2008). *Truth, Lies and Trust on the Internet*. Routledge.

Wiles, R. (2012). *What Are Qualitative Research Ethics?* A&C Black.

Wilhelm, A.F.X. and Kestler, H.A. (2016). *Analysis of Large and Complex Data*. Springer.

Wilkinson, S. and Kitzinger, C. (2013). Representing Our Own Experience: Issues in "Insider" Research. *Psychology of Women Quarterly*. 37 (2), 251–255.

Williams, M. and Levi, M. (2012). Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors. *Security Journal*28:252–271.

Williams, M.L., Burnap, P. and Sloan, L. (2017). Crime Sensing With Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns. *The British Journal of Criminology*57:320–340.

Williams, M. L. et al. (2018). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior*. 1–13.

Williams, P. and Vlassis, D. (eds.) (2001). *Combating Transnational Crime: Concepts, Activities and Responses*. Routledge.

Winner, L. (1993). Upon opening the black box and finding it empty: Social constructivism and the philosophy of technology. *Science, Technology & Human Values*.

Witkin, S. (2011). *Social Construction and Social Work Practice: Interpretations and Innovations*. Columbia University Press.

Witten, I.H. and Frank, E. (2005). *Data Mining: Practical Machine Learning Tools and Techniques, Second Edition*. Morgan Kaufmann.

Yang, Q., Hu, X., Cheng, Z., Miao, K. and Zheng, X. (2014). Based Big Data Analysis of Fraud Detection for Online Transaction Orders. In: *Cloud Computing*. Springer, Cham, pp. 98–106. Available at: https://link.springer.com/chapter/10.1007/978-3-319-16050-4_9 [Accessed: 13 April 2017].

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*. 2 (4), 407–427.

Yar, M. (2013). *Cybercrime and Society*. SAGE.

Yin, R.K. (2015). *Qualitative Research from Start to Finish, Second Edition*. Guilford Publications.

Youngblood, J.R. (2015). *A Comprehensive Look at Fraud Identification and Prevention*. CRC Press.

Ziemkendorf, M. (2008). *Actor-Network Theory*. GRIN Verlag.

Zwitter, A. (2014). Big Data ethics. *Big Data & Society*1:2053951714559253.