MASTER THESIS

The implications of fraud committed against enterprises in the Netherlands

Vulnerabilities, damages, consequences and prevention

May 2018

Marleen Schlömer

MSc. Business Administration
University of Twente

Information page

Colophon	
Document type	Master Thesis
Title	The implications of fraud committed against enterprises in the Netherlands
Subtitle	Vulnerabilities, damages, consequences and prevention
Version	Final version
Number of pages	56
Publication date	1st of May 2018

Credentials	
Author	Marleen Schlömer
Student number	s1490117
E-mail address author	m.schlomer@student.utwente.nl

Associated Study	
Educational programme	Business Administration
Track	Financial Management
Faculty	Faculty of Behavioural, Management and Social Sciences
Educational institution	University of Twente.

Examination board	
First Supervisor	Prof. Dr. M. Junger
Second Supervisor	Dr. S. Zubair

Preface

This is a master thesis on fraud at Dutch enterprises titled: The implications of fraud committed against enterprises in the Netherlands. This thesis was written in the context of a graduation project of the master program Business Administration at the University of Twente. From November 2017 up until April 2018, I have been working on this master thesis. The progress of my thesis had its ups and downs over this period of time, but nonetheless this always resulted into new ideas and alternative perspectives.

In search for a dissertation topic a came across an announcement by Prof. Dr. M. Junger. We made an appointment, and once talking I immediately became interested in the fraud phenomenon. One thing led to another and before I knew it, I had a very interesting and challenging research topic on my hands. The graduation process has been an educative one, in which I have applied the knowledge and skills that I have learned during my study. Next to putting knowledge and skills into practice, I have also gained new insights and developed myself personally as well as professionally.

This thesis, and there with the completion of my study, would not have been possible without the support and guidance of my supervisors, family and friends. Firstly, I would like to thank my first supervisor Prof. Dr. M. Junger for her guidance and feedback, which she has always provided with enthusiasm and expertise. Her active involvement, patience and pleasant manner of supervising have helped me during the entire process. Secondly, I would like to thank my second supervisor Dr. S. Zubair and external supervisor Jos Kerssen for their support during my graduation period.

Lastly, I would like to thank my friends and family for their motivational support and understanding during the past half year. They have motivated and encouraged me at the right times, which has helped me finish the thesis the way I did. I am very positive about my final thesis and I hope you feel the same. I hope you will enjoy reading my thesis.

Marleen Schlömer

Enschede, 1st of May 2018.

Abstract

The chance that fraudsters are caught is around 1%, whereas the overall damage of fraud in the Netherlands is estimated to be more than 10 billion euros. Therefore, this research aims to shed light on fraud targeted against companies. This paper discusses the differences amongst acquisition fraud, CEO fraud and ghost invoices with regards to fraud and company characteristics and to what extent these characteristics have an effect on financial damage and fraud successfulness. The goal is that the results can be used to establish preventive measures that will help in the fight against fraud. Fraud notifications on three types of fraud are gathered from the Fraudehelpdesk (FHD) and processed into a dataset with the use of a coding scheme. Of each type of fraud, one-hundred fraud notifications are gathered and processed. In order to draw proper conclusions, the data is supplemented by data from Statistics Netherlands on the economic landscape of companies in the Netherlands. The data is quantitatively analysed with the use of cross tabulations and regression analyses.

The results show that there are many differences between the three types of fraud. There are for example seasonality and size effects. Acquisition fraud is mostly attempted in winter and against self-employed and micro companies. Ghost invoices are mostly attempted in spring and against micro and small sized companies. CEO fraud is mostly attempted in summer and against small and medium sized companies. In addition, our results indicate that companies that are targets of CEO fraud have the highest risk with regards to financial damage, followed by acquisition fraud and ghost invoices. Results suggest that the more effort fraudsters put in a fraud attempt, the higher the amounts asked and received when successful. Whereas most attempts are directed towards the tertiary sector, the chance of success is higher in the primary and secondary sector making the sector rather vulnerable. With these insights, and knowing the modus operandi of fraudsters, companies can focus more on their vulnerabilities.

Keywords: CEO fraud, acquisition fraud, ghost invoices, company characteristics, fraud characteristics, financial impact, fraud successfulness.

Table of Contents

Tables and figures

1. Introduction

Companies see fraud as one of the biggest risks to their company. Research suggests that they have reason to, since it seems that fraudsters are actively defrauding businesses, especially with regards to acquisition, invoice and CEO fraud (Accura, 2017). Accura (2017) shows that especially young business owners are targeted, as they are inexperienced and do not have the time and money to properly protect their business yet.

What is daunting when it comes to fraud is that it has rapidly become more sophisticated, making it extremely difficult to track or catch fraudsters. This is also shown in the statistics of the Netherlands. Here it becomes evident that although the fraud rates go up the number of solved fraud crimes stays the same or even declines (Statistics Netherlands, 2017). Apart from the fact that fraud has become more sophisticated, globalization has also strongly enabled fraud. It is incredibly hard to catch a fraudster that commits fraud in the Netherlands whilst staying on another continent like Asia or Africa.

Another big enabler for fraud is technology, a large number of fraud attempts takes place via the internet. In 2015, one in nine people were exposed to a form of cyber-enabled crime in the Netherlands (Statistics Netherlands, 2017). There is a cat-and-mouse game going on between the offender and investigator. Offenders quickly learn about new technologies and exploit these while investigators catch up and then use the same technologies to investigate and apprehend offenders and eventually prevent future crimes. New technologies and opportunities to commit fraud emerge more and more rapidly and these opportunities quickly turn into a crime wave, potentially causing enormous damage for individuals and organizations (Wall, 2007).

Fraud is a so-called umbrella concept under which many form of fraud are present. Fraud comes in many shapes and sizes and it is therefore extremely difficult to get a complete image of what role fraud plays in the present day. As mentioned in the previous paragraph fraudsters continuously change and adapt their techniques, which next to globalization plays a major part in the opacity of fraud. This makes it also hard for authorities to protect their citizens and organizations from fraud. Authorities are constantly weighing between better protection for their citizens on the one hand and privacy of the offender on the other hand.

A recent article in the Dutch Financial Newspaper (de Lange, 2017) about a new project called the FraudInfodesk provides insights into the privacy problem. The project, which is a joint effort between the University of Twente and the Fraudehelpdesk, makes cross-sectoral information sharing possible. When an offender does not pay his phone bill, the phone company can send the personal details of that person to the FraudInfodesk, which then shares it with other possible targets. The argument here is that is sometimes necessary to not provide offenders with the same right of privacy as other people, because otherwise we will never be able to keep up with them.

1.1 Problem Definition

According to estimations fraud costs the Netherlands around 30 billion euros per year. Of this estimation around 55% is fraud committed against the government, 45% is fraud committed against companies and a mere 5% is fraud committed against private persons (Schalke &

Partners, 2014). Looking at government fraud various fraud detection systems are in place, investigations are being done and measures are taken. This is easier as the government exists out of far less organizations than the corporate world in the Netherlands. In order to reduce fraud against companies extensive research and collaborations, like the FraudInfodesk, are necessary.

Existing research on fraud against companies focuses mostly on large corporations and multinationals and less on companies in general. Accura (2017) for example found that among their respondents (large financial institutions) CEO fraud has the largest financial impact on their customers, invoice fraud is most frequently seen and acquisition fraud is most difficult to identify and/or counteract. In addition, they find that for businesses keeping up with the constant changes in fraud is very difficult and that awareness within a company is very important in preventing fraud. Bloem & Harteveld (2012) find that common denominators in most types of fraud targeted at companies are mass marketing fraud and identity fraud. Interesting in their research is that they state that the trust in a righteous society is at stake when we let fraud rampant, which is also supported by the research of van Geldrop & de Vries (2015). The most important factor that maintains fraud against companies is the high earnings and low risks for fraudsters which makes the chance of getting caught extremely low. Duffield and Grabosky (2001 & 2001) describe that this is the main reason which makes people commit fraud.

It is astonishing how little research has been done on fraud targeted against companies, especially since the internet makes companies more vulnerable and easier to defraud. Companies mostly have an online presence, where contact details of for example employees are easily found. Junger et al. (2013) found that 41% of fraud cases are digital and that ICT plays a greater role in fraud than people assume. As fraudsters become more and more innovative in their use of ICT, companies become more and more vulnerable to fraud. In a paper by the European Federation of Accountants (2005), fraud targeted at companies is described as hard to quantify but nonetheless rapidly increasing in western EU countries, causing high financial damages and sometimes financial distress. What however misses in these researches is data on fraud at companies and the analysis thereof. This paper attempts to function as a guide to analyse fraud at companies and help limit the risks and prevent fraud.

1.2 Research Objective

The aim of the present study is to shed light on fraud targeted against companies. As acquisition fraud, CEO fraud and ghost invoices are the types of fraud that occur most, the present study will focus on these three. Looking at the crime triangle it shows an interesting new angle. Where the perpetrator is interesting because when getting inside his head crimes can be prevented, it might also be of high value to focus on where the crime is committed. Especially looking at fraud at companies, as they are both the target and the place where the fraud is committed. Hence, the main objective of this research is to focus on all three aspects of the crime triangle, with a main focus on the target and the place. If barriers can be implemented that help take the aspects of the crime triangle out of the mix, the fraudster is unable to commit fraud. This can be because the fraudster is unable to attempt fraud or because companies recognize fraud attempts.

As mentioned before the companies that are especially vulnerable for fraud, are those that do not have the resources to keep up with the constantly changing approach and tactics of fraudsters. Especially Small and Medium-sized enterprises (SMEs) are more likely to suffer severe consequences due to fraud as they often do not have the resources to bounce back after fraud. In the current Dutch economic landscape, SMEs are crucial as they make up around 99% of all companies and 70% of all employed people work in a SME (Statistics Netherlands, 2015). This gives rise to second objective of this research, which is to provide insights in how vulnerable companies are with regards to fraud, what the consequences are of fraud and how the risk and vulnerability of fraud can be reduced for companies.

An additional objective is to provide the Fraudehelpdesk with information on their current role in the fight against fraud against companies. The Fraudehelpdesk is the organization at which data will be collected on the three types of fraud committed against companies mentioned earlier. Their goal is to help prevent fraud, by making people and companies aware of the dangers and possibilities of fraud. In addition, they assist in what steps to take when fraud is committed, hence making sure it does not happen again. In analyzing fraud cases the objective is to provide the Fraudehelpdesk with feedback on their activities surrounding these fraud cases in order to improve them.

1.3 Relevance

This research has both practical and scientific relevance. As for scientific relevance, this study explores a gap in current literature because it focuses on all types and sizes of companies, the Dutch economic landscape. Where previous studies have focused on financial institutions or large companies this study encompasses a broad perspective. The main reason is that focusing on large companies or financial institutions is in contrast with the literature as SMEs are particularly vulnerable to fraud and that fraud committed against SMEs has a bigger impact on these companies than bigger companies. In order to explore fraud committed against companies, this research uses data gathered on fraud within the Netherlands.

In addition, a crime script will be identified which provides the steps a fraudster takes in attempting fraud. In combination with the date this can potentially result in preventive measures to prevent future fraud attempts. With crime scripts ICT programs can for example be developed that can easily spot patterns and detect fraud. In addition, weakness in the scripts might give rise to other barriers that may help prevent fraud. These two aspects relate to the practical relevance this research provides.

1.4 Structure

This paper is structured in the following way. First, a theoretical background is established in chapter 2. In chapter 3, the research question is posed, and hypotheses are formulated substantiated with previous literature and empirical evidence. Then the research design is described in chapter 4 by walking through the dataset and sampling, research methods, and operationalization. In chapter 5, the results of the analyses are formulated and described. This leads to the discussion, conclusion and recommendations in chapter 6.

2. Theoretical Background

In order to understand what this research will incorporate, the concepts surrounding fraud and theories describing the reasoning behind fraud will first be defined and explained. It is important to define the concepts and theories that will be used in the research because in this way misunderstandings about the concepts and/or theories can be prevented and it is abundantly clear what is meant with certain concepts and theories. The theoretical framework incorporates fraud in general and specifically fraud in which companies are victimized. Literature and empirical evidence will be discussed with regards to understanding fraud.

2.1 Fraud

Fraud is a very broad concept that can be defined and conceptualized in many ways. However in general all definitions attempt to describe the same phenomenon. This research will use the general conceptualization posed by Bloem & Harteveld (2012, p. 11) who state that fraud is *"An intentional act in which a fraudster uses false pretences as an advantage to benefit or enrich himself at the cost of others"*. In order for this act to be fraud Bloem & Hartveld (2012) pose that there need to be five factors present. These five factors are: a deceived person, intentional acting, unlawful or illegal acting, misleading representation of facts, and the potential of economic gain. If one of these five actors are not present the act cannot be described as fraudulent.

2.1.1 Vertical, Horizontal and Diagonal Fraud

Within the concept of fraud Bloem & Hartveld (2012) make a distinction between vertical, horizontal and diagonal fraud. Vertical fraud is fraud committed by a civil person at the expense of the government. There are two sides to vertical fraud, the first being when a civilian unlawfully receives something from the government like a subsidy, benefit or even an identification document. The second aspect is when a civilian should pay or give something to the government but commits fraud in the process. An example is when people change their tax return in order to pay less or receive more (Bloem & Hartveld, 2012).

Horizontal fraud is when individuals, companies or financial institutions or organizations are victimized by fraud. In this form of fraud the government plays no role and various types of fraud are present. A few examples of types are acquisition fraud, mortgage fraud, insurance fraud and online trading fraud. This form includes fraud committed against individuals as well as companies and fraud committed by individuals as well as for example crime unions (Bloem & Hartveld, 2012).

Diagonal fraud is a hybrid form in which vertical fraud is mixed with horizontal fraud. Examples of types of fraud are bankruptcy fraud and identity fraud. The reason for these types to be called diagonal fraud is because civilians and companies but also the government can be victimized due to this form of fraud (Bloem & Hartveld, 2012). The present study focuses solely on horizontal fraud, in particular fraud committed against companies.

2.1.2 Structured and Unstructured Fraud

Another distinction that can be made within the concept of fraud is whether the fraud is structured or unstructured. Fraud is structured when there are people structurally working together in committing fraud and with the purpose to jointly gain financially or materially. In

most cases characteristics of these fraudsters are that they have a certain amount of organisation, commit fraud frequently and repeatedly and cause a substantial amount of financial damage at their victims. Unstructured fraud, as the name suggests, is the opposite of structured fraud. Unstructured fraud shows no patterns, no groups that frequently work together and causes (on average) less financial damage. As the present study focuses on fraud committed against companies, the focus is on structured fraud (Bloem & Hartveld, 2012).

2.2 Types of Fraud

Within fraud various types can be distinguished, we will use the types of fraud as suggested by the Fraudehelpdesk (hereafter: FHD) in their "Manual Types of Fraud" (Fraudehelpdesk, 2017). This research focuses on acquisition fraud, ghost invoices and CEO fraud as these are the types of fraud that are most popular when it comes to fraud committed against companies. The three types of fraud that will be studied in this research will be discussed next.

By sending a ghost invoice a fraudster tries to make a company pay for a service or product which they did not actually buy or request. The fraudsters draws up a ghost invoice which reflect a service and/or product a company is likely to buy and then send them to hundreds if not thousands similar companies at once. The invoice then becomes one of many invoices a company receives, making it easier for a ghost invoice to be accidentally paid. In 2016 there were 3204 cases reported at the FHD pertaining ghost invoices.

Acquisition fraud is defined as: "The false acquisition of advertisement/listing assignments in papers or websites". Fraudsters that engage in this type of fraud contact companies via post, email or telephone. They convince the company to agree to buying a service or product by recording a telephone conversation or making a company sign an agreement. Without knowing it the company has then agreed to a subscription of several months and are being send invoices. In 2016 there were 1293 cases of acquisition fraud reported at the FHD.

With the last type of fraud, CEO fraud, a fraudsters pretends to be the CEO of a company. Employees (mostly of the financial department) are contacted and asked to transfer a large sum of money in order to pay for something. This mostly happens via email where the mail of the CEO is hacked, spoofed, or mimicked. In 2016 there were 136 cases reported at the FHD pertaining CEO fraud.

2.3 Damage due to fraud

In all types of fraud, the goal of the fraudster(s) is to gain at the expense of another. This gain is almost always financial but the cost to the defrauded party is not always solely financial. This cost, varies with every fraud case and amongst types of fraud. Looking at the damage that can be done by fraud a distinction can be made between two types of damage: image and financial damage. Financial damage is defined as economic loss that the defrauded party suffered due to the fraud, whereas image damage is defined as loss of credibility or face the defrauded party suffered due to the fraud. The latter can for example be when a fraudster uses the name of a company in committing fraud. This can hurt the company as the defrauded parties think that that company committed the fraud. In reality, this was actually done by a third party, the fraudster.

Looking at acquisition fraud, CEO fraud and ghost invoices the damage the defrauded parties suffer are mostly financial. But even though image damage might not be defined economically, it can have financial impact. If the name of a company is damaged, customers or suppliers could not want to work with or buy from this company and that has a financial impact. This financial impact however, is extremely hard to objectively measure.

Looking at the data of the FHD the actual financial damage that was reported in 2016 of these three types of fraud, are as follows:

- CEO fraud: €587.544,-
- Acquisition fraud: €145.820,-
- Ghost invoices: €34.455,-

2.4 Understanding Fraud

As the previous paragraphs show, fraud can come in many forms and shapes, but how and especially why do people commit fraud? In order to understand people their reasoning with regards to committing fraud various theories and approaches are commonly used. This section discusses these theories and approaches in order to get a complete view of the concept. Starting with more general theories about the nature of people and then writing towards more specific situational theories which discuss criminal behaviour.

2.4.1 Nature of people theories

2.4.1.1 Rational Choice Theory

The rational choice theory assumes that all people are rational and therefore act rational. Friedman (1953) said that this rationality means that "an individual acts as if balancing costs against benefits to arrive at action that maximizes personal advantages". In order for the argument of Friedman (1953) to be true some assumptions are made within the rational choice model. These assumptions are: individualism, self-regard, and optimality. The assumption of individualism states that individuals are self-interested in the actions they take and in doing so they are only concerned with their own welfare, which is the assumption of self-regarding interest. Optimality refers to the assumption that individuals optimize their actions to have the most benefit (Abell, 1991).

2.4.1.2 Theory of Reasoned Action

Another theory that pertains to the behaviour of people is the theory of reasoned action (TRA). TRA states that the intention to show a specific behaviour is the best predictor of the actual behaviour of a person (Ajzen & Fishbein, 1980). In order to intent to act there are two factors that are of importance, attitudes and perceived social norms. Attitude points to the knowledge people have about the behaviour, as well as the evaluation and the consequences of the behaviour. Perceived social norms is decided by social norms, the observed behaviour of others and the pressure or support for a behaviour. Perceived social norms is subjective and can therefore be very different for different people. Looking at the TRA it is evident that again a trade-off is made, between the attitude towards a certain behaviour and the perceived social norms of the behaviour (Cornish & Clarke, 2008).

2.4.1.2 Theory of Planned Behaviour

It is unclear if attitude and perceived social norms are enough to fully predict behaviour. Therefore Ajzen (1991) added the concept of perceived behavioural control to the TRA model, establishing the theory of planned behaviour (TPB) shown in figure 1. It refers to the control a person believes he/she has over a behaviour, and it includes the level of difficulty required to perform the behaviour as well as outside factors at the belief whether these effect the person's control over the behaviour. The basis is the same as the TRA theory it however now also includes external factors and how a person perceives these external factors.

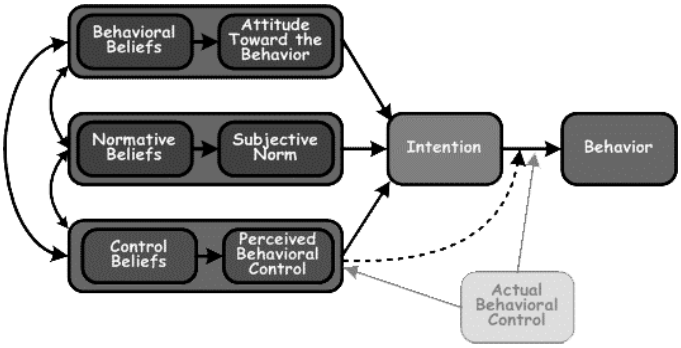

Figure 1: Theory of Planned Behaviour (Ajzen, 2006)

2.4.2 Situational Theories

2.4.2.1 Fraud Triangle

The theories mentioned in the previous paragraphs lead to the situations in which fraud can occur. This is described in a well-known concept called the fraud triangle. The fraud triangle is a conceptualization that tries to answer the "why" question that surrounds the concept of fraud and was established by Cressey (1950). The three concepts that Cressey identified as the fraud triangle are: perceived opportunity, rationalization and perceived pressure as is shown in figure 3. The reasoning behind the fraud triangle is that these three concepts are present in every case of fraud. In this sense perceived opportunity is the chance to act that the fraudsters sees with a low risk of being detected. Rationalization on its turn reflects the justification of the action before the action takes place. The perceived pressure completes the triangle, and stands for a pressure the fraudster is under which motivates him/her to commit the fraud. This perceived pressure mostly is financial and also non-shareable (Dorminey et al., 2012).

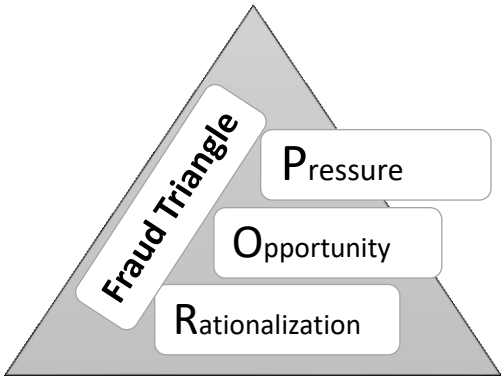

Figure 2: Fraud Triangle (based on Cressey, 1950)

2.4.2.2 Routine Activity Approach

The theories in the previous section focused on behaviour in general, but Cohen & Felson (1979) focussed on criminal behaviour and presented the routine activity approach. This approach emphasizes the circumstances in which offenders carry out criminal acts. The assumption that this approach is built upon is that crime can be committed by anyone, if that person has the opportunity to do so. In addition this approach also discusses the victims and state that victims have a certain choice not to put themselves in a situation where someone can commit a crime against them. Cohen & Felson (1979) stated that there are three conditions that need to be met in order for a crime to take place. There has to be a motivated offender, a lack of guardianship and lastly a suitable target.

Routine activities are patterns of activities that are present in a society, these patterns can for example be work, leisure or family related. The structure of these activities influence the situations that emerge and people also act in response to certain situations. The routine activity approach therefore poses that these routine activities determine for a large part the level of crime involvement of people. This approach is again linked with the rational choice theory as individuals come across opportunities to commit crime due to their routine activities and then make a rational choice (weighing benefits and costs) to decide whether or not to actually commit the crime (Cohen & Felson, 1979).

The routine activity approach is often depicted into a triangle which is called the Crime Triangle. The triangle (figure 3) has an inner and an outer triangle. The inner triangle shows the three elements that need to be present in order for a crime to potentially occur. The outer triangle lists controllers that are able to intervene on behalf of one of the three elements to prevent a crime (Cullen, Eck & Lowenkamp, 2002).

A potential target for example may be an employee in the financial department that automatically pays all incoming invoices without checking them. The guardian that can stop the employee from being a potential target might be the employee's executive who tells him to check all invoices and explain that not all invoices might be correct and genuine.

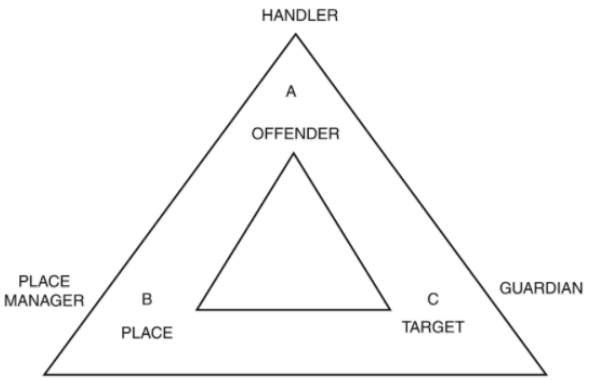

Figure 3: Crime Triangle (Cullen, Eck & Lowenkamp, 2002)

2.4.3 Crime Scripts

Where all these concepts and theories that help understanding fraud come together is in the concept of crime scripts. In 1994, Cornish proposed the idea of crime scripts in psychology. Using this concept he developed a framework that systematically captures all the aspects that a criminal needs in order to successfully commit a crime. The aspects range from equipment, to activities and locations and are a step by step plan from before to after the actual commitment of the crime. What was revolutionary about his approach is that he saw crime as a process instead of an event. Crime scripts can be seen as a set of decisions which form the modus operandi of crimes. When building up such a crime script from single actions a template is created which could reflect future behavior of a criminal or the sort of crime (Cornish, 1994).

3. Research Framework

In this section, the theoretical insights lead to a posed research question. This question will be split up into two parts, in part one the first part of the research question together with interesting thoughts and findings from literature will be combined into hypotheses. In part two, some background information relating to the second and third part of the research question will be translated into some expectations.

3.1 Research Question

The aforementioned theories show that analysing fraud is complicated and that many factors should be taken into account. It is interesting to look at the fraudster(s) perpetrating the (attempt to) fraud as the nature of people theories show that they are rational human beings that weigh costs against benefits and have intentions to act a certain way. It is however, at least as interesting to look at the victim of the fraud. As the fraud and crime triangle indicate, presenting offenders with the opportunity / place and target is also an aspect of crime that should be researched. Therefore this research tries to incorporate different perspectives, by looking at the victim as well as the perpetrator in analysing fraud and combining these perspectives in crime scripts. This leads to the following research question:

How do acquisition, invoice and CEO fraud differ amongst each other when looking at fraud and company characteristics? To what extent do fraud and company characteristics have an effect on financial damage and fraud successfulness? Can these insights, when combined with crime scripts, lead to preventive measures?

The first part of the research question will be answered by formulating and testing various hypotheses. These hypotheses reflect aspects of the fraud attempt itself, the targeted company and the outcome of the fraud attempt. In the next section, these hypotheses will be formulated, substantiated with theory. These hypotheses then lead to certain expectations for the second and third part of the research question.

3.2 Hypotheses

3.2.1 Fraud Characteristics

Looking at the crime triangle it becomes evident that a fraud is only possible when an offender has a suitable place and target. In addition, there is no handler present who can tell the offender not to commit fraud, no guardian who can tell the target no to engage, and lastly the place is not (properly) managed. But what happens when all of the aspects are in place that make fraud possible? How does the offender "engage" to commit fraud? This looks like an easy to answer question, but is more complex than it seems. The approach of a fraudster might differ with the type of fraud, the fraudster and the situation.

3.2.1.1 Fraud success

An attempt to commit fraud does not always leads to success. In the past years, the attempts have increased whilst the actual successful fraud attempts remained equal or decreased amongst types of fraud (Fraudehelpdesk, 2017). Whether or not the attempt is successful may depend on the fraudster, the company and external factors. If the fraudster does poor research on the company his attempt will more easily be uncovered than if he does excellent research. The company plays a role in making sure that its employees are aware of the potential dangers of fraud and keeping them up to date with developments. In addition, chance plays a role. If the attempted fraud is done in a period when it is really hectic at the company or when many employees are on holiday the chances of success are higher. Lastly, external factors such as government initiatives and organizations that play a role in identifying developments in fraud and increasing awareness have shown to have a positive effect on how many attempts are successful (Van Geldrop & De Vries, 2015).

Another interesting aspect of fraud successfulness is the scalability of the different types. Scalability refers to the amount of effort a fraudster puts into the fraud attempt, and according to the rational choice theory fraudsters are looking for low effort and high gains. Looking at the conceptualization of the different fraud types in the present study, one could expect that of the three types, CEO fraud has the lowest scalability, then acquisition fraud and ghost invoices has the highest scalability. The main reason for this is that once and invoice is made it is quite easy to change the company information to another company. Whilst on the other hand, CEO fraud requires more intensive contact between the fraudster and the company. As more intensive contact increases the chance of success, we arrive at the following hypothesis:

H1: The success rate of fraud attempts differs amongst types of fraud. CEO fraudsters experience the highest rate of success and ghost invoice senders the lowest rate of success.

3.2.1.2 Seasonality

Now, let us look into when fraud is likely to occur. Six decades ago Falk (1952) already researched the influence of seasons on crime rates. He found that crimes that have specific targets, such as people, are at a maximum in the summer months. In contrast he found that crimes against property, such as auto theft and burglary do not have specific moments in a year were they are at a high or low. In general he found peaks in criminality around the holidays in December and in the summer months. A more recent research by Hipp, Bauer, Curran & Bollen (2004) also found evidence for an increase in crime rates in summer. They found support for the routine activities approach suggesting that more pleasant temperature rates encourage people to spend less time indoors and more outdoors, which increases opportunities to commit crime or be victimized.

With regards to fraud the in- and outdoors does not matter too much as fraud is mostly perpetrated on a distance. However the fact that people are more and more busy with all sorts of activities in the summer months, could make fraud more likely to occur. As the internet becomes more and more extended, fraudsters are able to find contact information and also information on whether employees are away on for example summer holidays. Looking at the rational choice theory fraudsters try to achieve low effort and high success rates. When a company has a low occupation during the summer months the chances of success increase for the fraudster, hence the amount of fraud attempts should be higher during these months. As there is no empirical evidence on differences in seasonal patterns amongst types of fraud we do not distinguish between them. The abovementioned arguments give rise to the following hypothesis:

H2: Fraudsters are more likely to try and defraud a company during the summer than during the winter.

3.2.1.3 Financial damage

As mentioned fraudsters try their best to make their fraud attempt seem as real and genuine as possible, thereby enlarging their chances of success. If a fraud is successful their gain is the financial damage a company suffers. In attempting fraud, fraudsters determine the size of the potential financial damage by asking the company a specific amount of money when attempting the fraud. They want as high gains as possible but if they ask absurd amounts,

people get suspicious and the chances of success drop drastically. Therefore, the fraudster needs to weigh the chance of success against the potential gain if they ask a higher amount.

This makes it interesting to look at whether there are differences amongst types of fraud with regards to financial damage. As CEO fraud more often targets larger companies than acquisition fraud and ghost invoices one could easily make the assumption that the financial damage would tend to be higher as well. In the case of acquisition fraud the company is often trapped into a subscription for some months or a number of times, whereas on the other hand ghost invoices are a onetime payment of a product or service that was never bought and/or delivered. This would then suggest that ghost invoices concern a lower amount of money than is the case with acquisition fraud. This leads to the following hypothesis:

H3: The financial damage differs amongst types of fraud. It is the lowest when it concerns ghost invoices, a bit more when it concerns acquisition fraud and the highest when it concerns CEO fraud.

3.2.1.4 Identity of fraudster

The money the fraudsters ask need to be transferred to a bank account of someone or something. It is evident that fraudster want to preclude that they are caught. When it comes to fraud, especially the types this research incorporates, the identity of fraudsters are extremely hard to uncover. The reason for this is that fraudsters often use fake names and hide behind names of existing companies. This is fairly easy to do as sometimes all it takes is a fake name to make someone believe who you are (Grijpink, 2006). With the types of fraud in this research the fraudster either pretends to be someone else (CEO fraud) or use a fake name in combination with a real company (acquisition and invoice fraud).

The fraudster needs to set up a construction in such a way that the bank details match the personal details he uses in communicating with the companies. These bank details can either be on the name of a company or a person. It is however possible that the company which is used was incorporated in the name of a so-called money mule, these people have no idea that a company has been incorporated in their name. When the defrauded company reports the company that defrauded him the original fraudster has already defaulted the company and the money mule has no clue what happened in his name (Bloem, 2013). According to the rational choice theory, offenders weigh the costs against the benefits. When the real identity of an offender is unknown the costs drastically decline, a company name has lower risks than a real name. Although a company name might lead nowhere it is better than having no leads on the identity of the fraudster. This leads to the following hypothesis:

H4: Whether or not aspects are known about the identity of the fraudster does not differ amongst types of fraud as in most cases only the name of a (front) company is known.

3.2.1.5 Location of fraudster

If the name of a fraudster is hard to uncover, maybe the location is easier. If the police were to have the name of a fraudster and his/her location it would become easier to find a fraudster. Similar to the identity, the location of a fraudster is not always as easy to discover. Bloem (2013) points out that for many types of fraud, the criminal (organisations) are located in a different country than where the fraud takes place.

However, sometimes this is not the case. For example when, in order for the fraud to succeed, fraudsters need to seek personal contact with their victims, and hence need to speak the language, appear to be a national and/or have a company in the country. In the case of acquisition fraud and ghost invoices the sender of the ghost invoice needs to appear to have a company with which it is likely that the targeted company has an outstanding invoice, otherwise the employee is less likely to pay the invoice (Huisman & van de Bunt, 2009). Where, as mentioned, CEO fraud is thought to mostly target large companies this type of fraud seems to be much more established and bigger than the other two. In addition, large companies often do business across country lines, giving fraudsters an incentive to try and defraud companies in other countries (Zweighaft, 2017). Hence we arrive at the following hypothesis:

H5: The location of the fraudsters differ amongst types of fraud. Fraudsters are mostly located in the Netherlands with regards to ghost invoices and acquisition fraud, and outside the Netherlands with regards to CEO fraud.

3.2.2 The Company

3.2.2.1 Sector and Industry

Most of the fraudsters find their potential fraud victims on the internet, as this is much easier than driving around looking for companies. Focussing on the component internet, companies operating in the tertiary sector are more established on the internet than companies operating in the primary, secondary or quaternary sector, because they primarily provide services. One of the main focuses of service based companies is to maintain customer contact and provide services in a way the customer pleases. Whereas the main focus of a product based company is to provide the product the customer ordered (Lohrke, Franklin & Frownfelter-Lohrke, 2006; Levy & Powell, 2003). When a company is more active on the internet it is more likely to be found in general, including fraudsters. As service based companies have a lot of customer contact, fraudster can also easily find detailed contact information, making their fraud attempt easier. This is also in line with the rational choice theory, there is less effort for the fraudster, as the fraud attempt can be committed in less time when all the information needed can easily be found online. This argument leads to the following two hypotheses:

H6: Companies operating in the tertiary sector are more likely to be targets of fraud, than companies operating in the primary, secondary and quaternary sector.

H7: Companies operating in more service based industries are more likely to be targets of fraud, than companies operating in other industries.

3.2.2.2 Size

The most important motive for people to engage in committing fraud is the possibility of high earnings against relatively low risk. Fraudsters however have to weigh the risk of companies detecting the attempt of fraud against the amount to ask. If a fraudster asks an amount that is too low/high, the employee might get suspicious earlier then when he asks an amount that occurs more often. This suggests that the size of the company also matters as large companies are more likely to have high expenses than smaller companies.

In the case of CEO fraud the fraudster is dependent on the relationship between the CEO and his/her employees in the financial department. If the employees know the CEO fairly well the employees are more likely to get suspicious when the CEO writes them an email using a manner of speaking that is unusual. As the fraudster wants to keep the chance that he is detected as low as possible it is more likely that he contacts a large company as opposed to a smaller one, as the chain of command is more extensive in a larger company (Zweighaft, 2017). When it comes to acquisition and invoice fraud this is not the case as here the fraudster depends on his own persuasiveness and perseverance, and the naivety and inexperience (in detecting fraud) of the companies' employee(s). Smaller companies and its employees are less experienced and have less resources at their exposal to detect fraud (European Federation of Accountants, 2005). Hence we expect fraudster to again make a rational choice in choosing their target, leading to the following hypotheses:

H8: Large companies are more likely to be targets of CEO fraud, whereas smaller companies are more likely to be targets of acquisition and invoice fraud.

3.2.2.3 Location

In addition to size, location might also be an interesting consideration for fraudsters. Looking at the three types of fraud we are researching and the expected approach (paragraph 2.6.1.2) we do not expect the fraudsters to physically meet any of their victims. Location however still might be an interesting aspect of fraud. The most economically active region of the Netherlands is the so-called Randstad, which consists of the four largest Dutch cities and their surrounding areas. An interesting proxy for location thus might be the population density of certain (rural) areas (Andresen & Malleson, 2013). An argument for the contrary is that the Randstad is also the most developed region of the Netherlands, making it plausible that the companies that have knowledge about how to detect and prevent fraud are also located in this region (Lambregts, 2008). The latter however, might play a lower role than the former mentioned argument, hence the following hypothesis:

H9: Companies located in the western part of the Netherlands (Randstad) are more likely to be targets of fraud.

3.3 Expectations

3.3.1 The relationship of fraud and company characteristics with financial damage and fraud successfulness

In the previous section we discussed specific fraud and company characteristics and hypothesized their relationship with fraud and amongst types of fraud. A very important aspect of fraud is financial damage, which only occurs when a fraud is successful. As mentioned in the introduction fraudsters constantly adapt themselves making it hard for (smaller) companies to keep up. Hence, causing financial damages and sometimes even financial distress for companies (European Federation of Accountants, 2005). It is very hard to identify let alone catch and stop fraudsters, making it interesting to focus on the prevention of fraud. If we know the vulnerabilities of companies we could possibly put specific preventive measures in place that take away those vulnerabilities. Hence, we are interested in the relationship between those fraud and company characteristics and to which extent they

determine the financial damage and fraud successfulness. To our knowledge, this has not been researched before and therefore we do not hypothesize any specific outcomes.

3.3.2 Crime scripts

The previous sections covered specific aspects of fraud, but relating the outcomes to the modus operandi of fraudsters could be even more interesting. Thus, information about the series of steps a fraudsters takes in attempting to commit fraud. A crime script captures all these aspects and is a combination of all kinds of information (Cornish, 1994). An emerging method in trying to understand crimes and developing barriers is crime script analysis. A crime script could assist in the prevention of fraud as well as the capture of fraudsters. When crime scripts are written on specific types of fraud these could help people and companies in becoming more aware with how fraud is committed and what to pay attention to. In addition, crime scripts could help in finding out which barriers are effective in preventing fraud. It does this by identifying points at which action, often in the form of barriers, can be taken.

Cornish (1994) originally applied crime script analysis to robberies, graffiti, and auto theft. More recently, crime script analysis has been applied to sexual assaults (Beauregard et al., 2007; Leclerc et al., 2011), organized crimes (Hancock & Laycock, 2010) and the online black markets (Hutchings & Holt, 2014). This research attempts to apply the concept of crime scripts to fraud (attempts) committed against companies.

4. Research Design

4.1 Dataset and sampling

This research uses secondary data from the database of the Fraudehelpdesk (FHD) and Statistics Netherlands. The latter functions as giving insights into the situation of companies in the Netherlands in 2016. The former, data from the FHD, is used in order to develop a dataset that contains all the data in order to be able to test the hypotheses posed in the previous chapter. As mentioned, fraud is a constantly changing phenomenon. This means in order to draw conclusions that can lead to practical implications it is interesting to study the most recent fraud notifications. The data that will be used for this data will be data from the FHD database from 2016. The reason for this is that the year 2017 was not yet over when this research started, which would mean that drawing conclusions about fraud in the year 2017 was not possible.

The FHD is the national helpdesk at which people and organizations can report fraud. The FHD processes these notifications into their database and if necessary refers the defrauded people to the correct institutions. The FHD is available to help people but also plays a significant role in learning more about fraud and the role and impact thereof in the Netherlands. Additionally, the FHD also offers some extras, this is in particular available to organizations. There is additional information on their website and in documents which they distribute, concerning the types of fraud organizations encounter. Furthermore, organizations can become a member and therewith get legal help and (preventive) advice from professionals.

What makes this is data from the FHD so interesting is that the FHD is the only organization in the Netherlands that gathers a large quantity of information on fraud. The FHD was founded in 2003 and over the last few years their database has grown extensively as they are gaining

more and more publicity. The notifications that are in the FHD database come from private persons and companies and are mostly in Dutch, which makes the database suited for a study pertaining the Netherlands. The FHD dataset contains a lot of detailed information on cases of fraud making it interesting to analyze this dataset in particular.

As mentioned, this research focuses on three types of fraud that companies encounter. For each type of fraud one-hundred cases are randomly selected from the FHD database for analysis. This is done with the use of the website www.random.org, in total three sets of 100 random numbers are generated. For each specific type of fraud this means that from the 136 cases (CEO fraud), 1294 cases (Acquisition fraud), and 3205 cases (Ghost invoice) in 2016 one-hundred are randomly selected.

4.2 Research Method

The data of the FHD was translated into English and processed into a coding scheme which can be found in appendix 1. Based on the coding scheme data will be collected and processed into a new dataset in IBM SPSS. The coding will be done at the FHD to guarantee the confidentiality of the data. Only the anonymized dataset has left the FHD and this is the only dataset that will be analyzed.

The data will be analyzed according to the mixed methods model, meaning that both quantitative and qualitative techniques are used. First, descriptive statistics will be produced to describe the overall dataset. These statistics will be supplemented by some data on the economic landscape of companies in the Netherlands. This gives a bit more insight in the situation in the Netherlands in 2016, hence functioning as a basis for interpreting the analyses.

Secondly, the crime scripts of the three types of fraud will be drawn up. This is done by qualitatively analyzing the FHD documents that describe the modus operandi of the types of fraud. This analysis is processed into the scenes and actions framework (appendix 2), which is filled out for every type of fraud. In doing this analysis a specific fraud attempt will also be described to provide a more practical insight into the modus operandi. This is done before quantitatively analyzing data because it gives more insight into the three types of fraud analyzed in the present study.

In order for us to be able to answer part one and two of the research question quantitative analyses will be performed. An overview thereof can be found in the analytical framework in figure 4. In order to test the posed hypotheses (relationship one and two in figure 4), bivariate analyses are performed by producing cross tabulations. These cross tabulations will provide the results needed to either reject or accept hypotheses. The second part of the analyses focuses on finding additional relationships between the variables (relationship three in figure 4), and to this purpose two multivariate regressions are run. The first multivariate regression is a multiple regression, which is run to test the relationship between company and fraud characteristics and financial damage as a result of the fraud attempt. The second multivariate regression is a binary logistic regression, which is run to test the relationship between company and fraud characteristics and fraud successfulness.

Both multivariate regressions contain two models, the first model assesses relationship three from the analytical framework and the second model additionally tests the possible mediating role of the types of fraud.

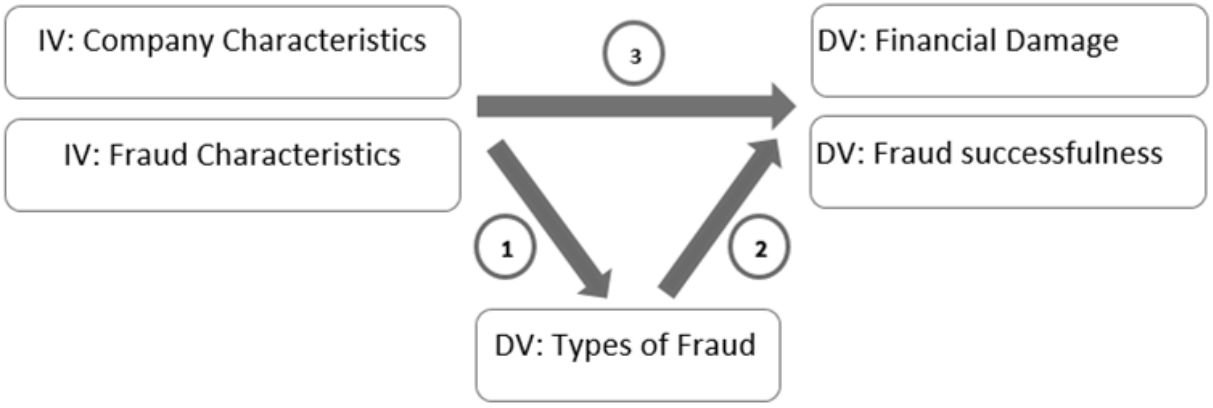

Figure 4: Analytical Framework (Schlömer, 2018)

4.3 Operationalization

In this paragraph, the variables derived from the data and their operationalization are discussed. The operationalization of these variables go hand in hand with the coding scheme but will shortly be explained in more detail. As mentioned, this research focuses on three types of fraud. These three types were conceptualized in chapter 2 by the definitions that the FHD uses in order to categorize notifications. As these notifications are the primary data source for this research the operationalization of the types of fraud the FHD uses were used for this research. As some of the variables are categorical, dummies were created in order to run regressions. In each regression model one dummy will be left out of the analysis, making it the reference category.

4.3.1 The Fraud

The fraud (attempt) pertains the timing of the fraud, the monetary aspect and whether or not the fraud was successful. They are all operationalized by reading the information and documents the defrauded company has provided in the notification. As for the timing of the fraud the date the fraudster first contacted the company was selected. In addition, the amount requested by the fraudsters was noted. Whether or not the company actually paid this amount and noticed it was an attempt to commit fraud, this determines if the fraud was successful.

An additional aspect about the fraud (attempt) is information that can be found with regards to the fraudster, is his identity and location. These are both operationalized with the use of the bank detail the fraudster provided whilst attempting the fraud. The identity of the fraudster pertains to the name of the person or company mentioned with the bank details. The location of the bank determines the location of the fraudster and was noted as both country and continent.

4.3.2 The Company

Dutch companies dealing with (an attempt of) fraud are the main focus of this research and incremental are their company characteristics. Our sample contains self-employed, SMEs, large and extremely large companies. Within the sample a company was classified as an SME when it has between 2 and 250 employees, large when it has between 251-1000 employees and extremely large when it has more than 1000 employees.

An overview of the company characteristics that will be used in analysis are:

- Sector (primary and secondary, tertiary, quaternary)
- Industry (SBI-2008 code)
- Size (categories and FTE)
- Location (province and city).

A more extensive operationalization of all variables can be found in the coding scheme (appendix 1).

5. Results

5.1 Descriptive Statistics

In order to get a general overview of our data descriptive statistics were generated (table 2). Looking at the descriptive statistics (table 2a), it is interesting to see that overall only 8% of the fraud attempts is successful. This is positive for the battle against fraud of course, but as one of our dependent variables is financial damage this percentage of cases is rather low. Therefore, we decided to use the amount asked by fraudsters instead of damages as a dependent variable. This variable is a good substitute for damages since the only difference between amount asked and damages is whether the fraud was successful or not. In our data we see that when the fraud was successful the company paid the amount asked.

Going back to our descriptive statistics, we see that spring and summer are periods in which most of the attempts take place, most fraudsters are located in the Netherlands, and the amounts asked by the fraudsters varies wildly. Concerning the companies that are targeted the descriptive statistics (table 2b) show that most companies operate in the tertiary sector and range between being self-employed to medium sized (max. 250 employees). Lastly, we see a huge variation in the industry in which the company operates and the province in which it is located.

Table 2a:
Descriptive Statistics: Fraud characteristics

	Total	%		Total	%
Fraud successful					
Yes	24	8%			
No	276	92%			
Timing of fraud			**Fraudster location**		
Winter	55	18.3%	The Netherlands	172	63.5%
Spring	106	35.3%	Europe (except NL)	61	22.5%
Summer	99	33%	Asia	25	9.2%
Autumn	39	13%	America	13	4.8%

Amount asked			Fraudster known		
0-200	75	33.3%	Yes, name	5	1.6%
200-400	27	11.8%	Yes, company	266	88.6%
400-10000	53	23.2%	No	4	1.3%
10000-75000	27	11.8%			
>75000	45	19.7%			

Table 2b:
Descriptive Statistics: Company characteristics

	Total	%		Total	%
Sector			**Size company**		
Primary and Secondary	75	25%	Self-employed (1)	70	23.3%
Tertiary	205	68.3%	Micro (2-10)	84	28%
Quaternary	19	6.3%	Small (11-50)	59	19.6%
			Medium (51-250)	54	18%
			Large (251-1000)	19	6.3%
			Very large (1000+)	13	4.3%
Industry			**Location**		
Agriculture, forestry and fishing	10	3.3%	Groningen	10	3.3%
Industry	31	10.3%	Friesland	7	2.3%
Construction	32	10.6%	Drenthe	10	3.3%
Wholesale and retail trade, repair	50	16.6%	Noord-Holland	66	22.1%
Transport and storage	14	4.6%	Flevoland	2	0.7%
Accommodation and food service	12	4%	Overijssel	16	5.4%
Information and Communication	17	5.6%	Gelderland	40	13.4%
Financial institutions	9	3%	Utrecht	19	6.4%
Renting, buying and selling of real estate	6	2%	Zuid-Holland	62	20.7%
Business Services	65	21.6%	Noord-Brabant	46	15.4%
Public services	0		Zeeland	9	3%
Education	6	2%	Limburg	12	4%
Human health and social work activities	25	8.3%			
Culture, sports and recreation	10	3.3%			
Other service activities	12	4%			

When looking at the descriptive statistics we see that there is a lot of variation amongst the company characteristics. This is not necessarily mean that certain types of companies are more likely to be targets of fraud, as this could also be a reflection of the economic landscape of the Netherlands. The variation amongst the provinces for example, does not necessarily mean that fraudster specifically target companies in certain provinces. The descriptive statistics that we see could also be the result of how companies are located throughout the

Netherlands. If in one area there are way more companies than in another, it would be logical that the area with more companies is targeted more.

In order to get a better view of the situation in the Netherlands we gathered data from the Statistics Netherlands (Statistics Netherlands, Bedrijfsleven, 2018). With regards to provinces we collected data on the revenue of all Dutch companies per province in the year 2016. Revenue is a good predictor of the size of economic activity, all revenue of the Netherlands in 2016 is allocated amongst the provinces in which the companies generating revenue are located. All twelve provinces combined add up to one hundred percent. Looking at our data (table 3), we see that in the case of our data the size of economic activity per province corresponds to the number of fraud notifications per province. In some cases the percentages are even within 0.2% of one another, and in the maximum case the difference is 5%.

Table 3: Percentage of fraud notifications and revenue of 2016 per province

Provinces	% Fraud notifications 2016 Netherlands	% Revenue 2016 Netherlands
Groningen	3.3%	1.9%
Friesland	2.3%	2.1%
Drenthe	3.3%	1.6%
Noord-Holland	22.1%	22.5%
Flevoland	0.7%	1.9%
Overijssel	5.4%	4.8%
Gelderland	13.4%	9.4%
Utrecht	6.4%	6.7%
Zuid-Holland	20.7%	25.7%
Noord-Brabant	15.4%	15.9%
Zeeland	3%	1.8%
Limburg	4%	5.6%
Total	100%	100%

Data: Fraudehelpdesk and Statistics Netherlands (Bedrijsleven, 2018)

Unfortunately we could not find the revenue of Dutch companies divided by industry or company size. Therefore we used the number of companies in the Netherlands as a reflection of the Dutch economic landscape with regards to industry and company size. The data with regards to number of companies was collected from the statistics of the Netherlands (Statistics Netherlands, Bedrijven, 2018). In table 4, we see that globally our percentages of fraud notifications per industry matches those of statistics Netherlands. With the business services industry being the largest group, then wholesale and thirdly construction. The largest difference is in the industrial industry, whereas more than ten percent of the fraud notification originated from this sector only four percent of all Dutch companies operate in this industry.

Table 4: Percentage of fraud notifications and Dutch companies in 2016 per industry

Industries	% Fraud notifications 2016 Netherlands	% companies 2016 Netherlands
Agriculture	3.3%	4.4%
Industry	10.3%	4%
Construction	10.6%	9.9%
Wholesale	16.6%	13.7%
Transport & Storage	4.6%	2.5%
Catering	4%	3.3%
Information services	5.6%	5.3%
Financial instit.	3%	5.4%
Real estate	2%	1.6%
Business services	21.6%	24%
Public services	0.0%	0.1%
Education	2%	4.8%
Health & Social work	8.3%	8.8%
Culture, sports & recr.	3.3%	6.2%
Other service activities	4%	6%
Total	100%	100%

Data: Fraudehelpdesk and Statistics Netherlands (Bedrijven, 2018)

In table 5, the percentage of companies in the Netherlands is shown divided amongst company sizes. Here we see that there is a large difference in the self-employed group, whereas around 23% of the notification originated from this group, almost 80% of Dutch companies fit into this group. If we however take self-employed out of the analysis, we see that both the fraud notifications percentages and the company percentages decrease when the company sizes increase.

Table 5: Percentage of fraud notifications and Dutch companies in 2016 per company size

Company sizes	% Fraud notifications 2016 Netherlands	% companies 2016 Netherlands
Self-employed (1)	23.3%	79.1%
Micro (2-10)	28%	16.9%
Small (11-50)	19.6%	3.1%
Medium (50-250)	18%	0.7%
Large (250+)	10.6%	0.2%
Total	100%	100%

Data: Fraudehelpdesk and Statistics Netherlands (Bedrijven, 2018)

5.2 Crime Scripts

Based on the theoretical framework and data analysis, crime scripts can be established. All three typed of fraud researched in this study have very straight forward modus operandi of which fraudsters seldom deviate. In combination with the gather data this leads to the crime scripts per type of fraud described in table 7. The crime script of LeClerc & Wortley (2013) was used as a basis for the crime scripts of the types of fraud discussed in the present study.

With all three types of fraud the first step a fraudster takes is the decision to attempt fraud and whether or not to do it alone or with co-offenders. In order to make such a decision the fraudster(s) must have assessed, referring to the rational choice theory, that the benefits outweigh the costs. The next step is the selection of the victims, which are in our case companies. Once these are selected the fraudster(s) need to do research on the companies, in order to come across as credible once they make contact. In the case of CEO fraud the research needs to be extensive, because the fraudster is posing as the CEO so he is ought to know certain things. In the case of acquisition fraud and ghost invoices extensive research is unnecessary, as the most important thing with these two types is knowing the company's type of business and contact information.

Where the previous steps were comparable amongst fraud types, the next steps differ amongst types. Where the next steps for ghost invoices is merely drawing up and sending of the ghost invoices and then waiting until they get paid, there is more extensive contact between the fraudster and target company with the other two types. In table 6, the approach types used in the fraud attempts in our dataset are shown split by type of fraud. The data in this table confirms that the crime script of ghost invoices is the most straight forward.

As for CEO fraud, the most common step after researching the company is spoofing the email address of the CEO. Spoofing an email address is done by making a slight change in the CEO's actual email address that is hard to spot. Examples are replacing a "0" with an "o" or a capitol "I" with a lowercase "l". The next step is the approach; the fraudster sends an email to an employee of the financial department whilst posing as the CEO. He then asks the employee to transfer a specific amount of money to a bank account. When the employee asks questions, he pushes the employee to make the transfer, often by mentioning that it has priority and that the paperwork can be arranged afterwards. As can be seen in table 6, some of the approaches in CEO fraud also occur via telephone. This approach is very rare, as the telephone number can be checked, fraudsters need to speak a specific language, and questions can easily be asked. This makes the chance of success much lower than via email.

The opposite is true for acquisition fraud, where most of the approaches happen via telephone (table 6). After doing some research on a company acquisition fraudsters approach a company by offering an interesting advertisement opportunity. There are two ways in which they try to get an employee to agree to the offer:

- They record a verbal agreement (via telephone)
- They send a contract which needs to be signed

In the case of the phone call, the employee is completely unaware that the phone call is being recorded, whereas in the case of the contract they willingly sign the contract. What then follows is a series of invoices that the fraudster sends to the company, which state that the

company has a subscription on the advertisement. When the company tries to contact the fraudster and explain that they never agreed to a subscription the reply of the fraudster depends on the type of agreement. In the case of the recorded phone call, the fraudster sends a (mostly tampered with) phone call recording, in which an employee agrees to a subscription. In the case of the contract, there is fine print hidden somewhere in the contract which states that once signed the company has agreed to a subscription. Worst of all is that often there never actually is an advertisement that is distributed.

Table 6:
Approach per type of fraud (CEO Fraud, Acquisition Fraud, and Ghost Invoices)

Type of approach	CEO Fraud	Acquisition Fraud	Ghost Invoices
Email	93	3	0
Post	0	9	100
Telephone	5	88	0

Table 7:
Crime Scripts per type of fraud (CEO Fraud, Acquisition Fraud, Ghost Invoices)

Script scenes	**Script actions CEO Fraud**	**Script actions Acquisition Fraud**	**Script actions Ghost Invoices**
Preparation	Decide to try and commit CEO fraud, possibly select co-offenders	Decide to try and commit acquisition fraud, possibly select co-offenders	Decide to send ghost invoices, possibly select co-offenders
Precondition	Look for and select potential company	Look for and select potential company	Look for and select potential company
Instrumental precondition	Do extensive research on the company	Do minimal research on the company	Do minimal research on the company
Instrumental initiation	Spoof the email address of the CEO	Approach the company and persuade the company to accept advertisement opportunity	Make an invoice for the company
Instrumental actualization	Contact the financial employee whilst posing as CEO of the company	Make sure there is an verbal or signed agreement	
Doing	Request a money transfer to a foreign bank account	Send invoices to the company per payment term	Send the invoice to the company
Post-condition	Push the employee to make the transfer	Push company to pay the invoices since there is an agreement	Hope that the company pays the invoice

5.3 Differences amongst types of fraud

The present research focuses on CEO fraud, acquisition fraud and ghost invoices. As the types of fraud differ, it is logical to also expect differences between the types of fraud with regards to the questions posed earlier. In order to look for these differences cross tabulations are generated to determine whether the differences amongst types of fraud are significant. The results will be discussed on the basis of the hypotheses posed in section 3.

5.3.1 Successfulness of fraud attempts

In hypotheses one we stated that fraud against companies is successful in less than 50% of the cases and that this success rate does not differ amongst types of fraud. Looking at the cross tabulation in table 4 we find no association between type of fraud and successfulness of fraud attempt ($X^2(2) = .295$, $p = 0.863$). With all types of fraud most of the fraud attempts were unsuccessful resulting in no significant difference between types of fraud. It is however interesting that in our dataset the fraud cases, amongst all types of fraud, were successful in less than 10 percent of the cases. Even though these types of fraud differ in for example type of approach and tactic of the fraudster there is no difference in success rate. As the success rate does not differ amongst types of fraud we reject hypothesis 1.

Table 8:
Cross tabulation of Successfulness of fraud attempt on types of fraud

	CEO Fraud	Acquisition Fraud	Ghost Invoice
Yes	9	8	7
No	90	92	93
N	99	100	100

Chi-Square= .295; df=2, p=.863
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

As mentioned in section 3.2.1.1 scalability might play a part in the successfulness of fraud. According to the rational choice theory fraudsters want low effort, low risk and high earnings. In order to see if that is possible for our sample, we crossed scalability with success rate for our three types of fraud. Scalability is shown on a scale of 1 to 5, where 1 means that the fraudster has put a lot of time in specifically targeting a victim and 5 means that the fraudster can attempt to defraud many companies with one fraud attempt. This is shown in figure 4, in addition the earnings the fraudster made per type of fraud are also shown. The successfulness of fraud attempts in our sample range between 7% and 9.1%. Figure 4 shows that CEO fraud has the lowest scalability in combination with the highest success rate and average earnings. In complete contrast with ghost invoices, which has the highest scalability of the three types but lowest success rate and average earnings. Where the average earnings extremely differ amongst the three types the average success rates are rather close. So even though we reject hypothesis 1 these results do show support in the direction of our hypothesis.

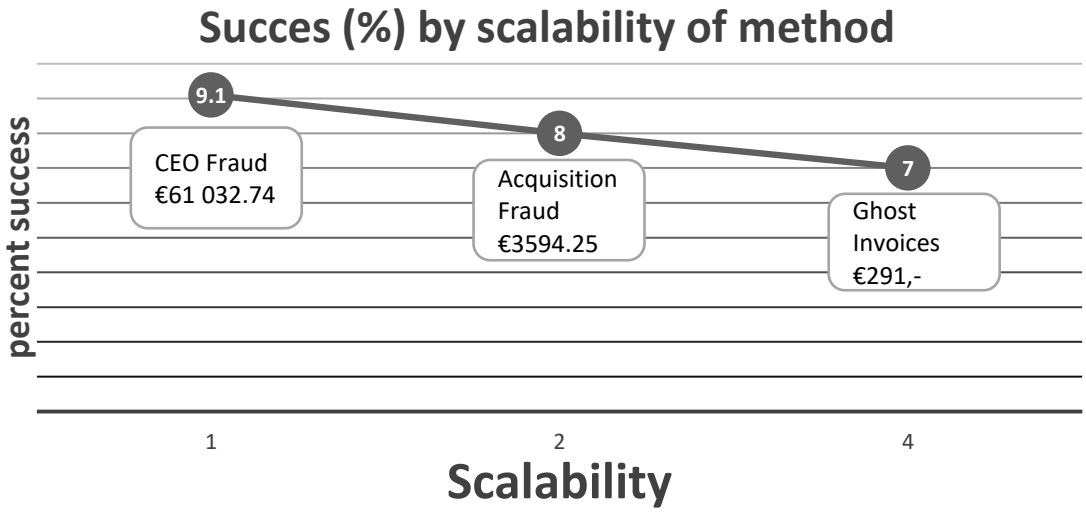

Figure 5: Success rate of fraud attempts by scalability of method and average earnings per successful fraud

5.3.2 Seasonality of fraud

This low success rate does not mean that fraudsters are not trying to achieve high success rates. As for the seasonality of the cases a distinction was made between four seasons, these four were put in a cross tabulation along with the types of fraud. In hypotheses 2 we stated that most cases of fraud occur during the summer months. Table 3 shows that there is an association between type of fraud and seasonality of fraud ($X^2(6) = 170.751$, $p = 0.000$). This means that the seasons in which the different types of fraud are attempted significantly differ amongst types of fraud. CEO fraud (attempts) mostly occur in summer, acquisition fraud (attempts) in winter, and ghost invoice (attempts) in spring. This means that we reject hypotheses 2. Whereas the stated hypothesis is true for CEO fraud, different seasonal trends are seen with regards to acquisition fraud and ghost invoices.

Table 9:
*Cross tabulation of seasonality of fraud on types of fraud****

	CEO Fraud	Acquisition Fraud	Ghost Invoice
Winter	6	32	17
Spring	5	29	72
Summer	73	18	9
Autumn	16	21	2
N	100	100	100

Chi-Square= 170.751; df=6, p=.000
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

5.3.3 Amount asked by fraudster

When we discussed the descriptive statistics, we already saw that the amount asked by fraudsters vary wildly. As this variable is a continuous variable we need to check for outliers that might influence the outcomes. To do this, frequency histograms were created per type of fraud for the amount asked by the fraudsters. These histograms (appendix 3) show that outliers are present in the groups CEO Fraud and Acquisition fraud. The histogram of CEO fraud shows one outlier of €425,000,00 and the histogram of Acquisition fraud shows two

outliers, one of €13,000 and one of €17,000. In order to account for these outliers the variable was recoded into five groups.

In a cross tabulation we tested whether the amount asked by fraudsters significantly differs amongst types of fraud. In hypotheses 3 we stated that CEO fraudsters ask the most, followed by acquisition fraudsters and ghost invoice senders. Looking at the cross tabulation our expectations are confirmed, with a statistical significance of .000 we confirm that the mean amount asked by fraudsters significantly differ amongst types of fraud, with the highest amounts asked in the cases of CEO fraud and lowest amounts asked in the ghost invoice cases. The amounts asked in the cases of acquisition fraud and ghost invoice lie close to one another whilst the amounts asked in the cases of CEO fraud are much and much higher. Hence we hereby accept hypothesis 3.

Table 10:
*Cross tabulation of amount asked by fraudster on types of fraud****

	CEO Fraud	Acquisition Fraud	Ghost Invoice
0-200	0	12	64
200-400	0	21	6
400-10000	0	24	29
10000-75000	25	2	0
>75000	45	0	0
N	70	59	99

Chi-Square= 270.716; df=8, p=.000
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

5.3.4 Identity of fraudster

With regards to the identity of the fraudster we hypothesized that for all three types of fraud only the name of a (front) company is known. Just like the location of the fraudster the identity is based on the bank account provided. We know based on the modus operandi and crime script that in communicating with the companies fraudsters use different personal names and company names. The money however, needs to be transferred to a bank account owned by someone or something. Looking at the cross tabulation (table 9) we find an association with type of fraud ($X^2(4)> = 24.812$, $p = 0.000$). As six cells have values of 5 or below 5, the ability to trust the output of the cross tabulation and validity thereof is low. Therefore, we can draw no conclusions on the basis of the table. If the assumption of expected count would be met, the results would be in line with what is already known, which is that fraudsters use the names of (front) companies in order to set up bank account and collect money. This way the real identity of the fraudsters become really hard to retrieve. We therefore accept hypothesis 4, but we will not use this variable in further analyses as there is no variation in output.

Table 11:
Cross tabulation of identity of fraudster on types of fraud

	CEO Fraud	Acquisition Fraud	Ghost Invoice
Yes, the name of the person(s)	5	0	0
Yes, the name of the company	66	100	100

No	4	0	0
N	75	100	100

Chi-Square= 24.812; df=4, p=.000. Assumption of expected count not met.
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

5.3.5 Location of fraudster

In hypothesis 5 we posed that there are differences amongst types of fraud with regards to the location of the fraudster. When we ran a cross tabulation with regards to the location of the fraudster, we found an association between type of fraud and location of fraudster ($X^2(4) = 234.740$, $p = 0.000$). As we had very few cases in which the fraudster's bank account was located in America we dropped it out of analysis. In doing so we get another significant association ($X^2(4) = 202.856$, $p = 0.000$). This (table 10) shows that the location of the fraudsters significantly differ amongst types of fraud. Whereas acquisition and ghost invoice fraudsters are mostly located in the Netherlands, CEO fraudsters are mostly located in the rest of Europe. With acquisition fraud there is no variation at all, whereas CEO fraudsters also originate in Asia and ghost invoice fraudsters elders in Europe. As we hypothesized that CEO fraudsters are located outside the Netherlands whereas acquisition fraudsters and ghost invoice senders are mostly located in the Netherlands we accept hypothesis 5. There is one side note however, there is no way of knowing if the location of the bank account always means that the fraudster is actually located there. Therefore, just like the variable about the identity of the fraudsters, this variable will not be used in further analysis.

Table 12:
*Cross tabulation of location of fraudster on types of fraud****

	CEO Fraud	Acquisition Fraud	Ghost Invoice
The Netherlands	1	100	71
Europe (except NL)	45	0	16
Asia	25	0	0
N	71	100	87

Chi-Square= 202.856; df=4, p=.000.
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

5.3.6 Sector of defrauded company

Besides information about the fraudster, our dataset also contains information about the companies that these fraudsters tried to victimize. With regards to the type of product or service a company sells or provides we have classified the companies into sectors and industries. In the cross tabulation (table 8) we see that the sectors are too broadly defined in order to find a difference amongst types of fraud. We find no association between type of fraud and sector ($X^2(4) = 5.895$, $p = 0.207$). We hypothesized that fraudsters mostly target companies in the tertiary sector. The results from table 11 show exactly that, fraudsters focus on the tertiary sector, then primary or secondary, and lastly quaternary. Hence, we accept hypothesis 6.

Table 13:
Cross tabulation of sector of defrauded company on types of fraud

	CEO Fraud	Acquisition Fraud	Ghost Invoice
Primary or Secondary	32	21	22

Tertiary	62	70	73
Quaternary	6	9	4
N	100	100	99

Chi-Square= 5.895; df=4, p=.207.
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

5.3.7 Industry of defrauded company

Subsequently, in hypotheses 7 we stated that fraudsters mostly target companies in service based industries. When we first ran the cross tabulation for industry we see that even though there is an association, the assumption of expected count is not met. The industries might be too specifically defined, so we tried to find a solution for this. When leaving the industries out of the analysis that are only occasionally present in the dataset, six industries remain (table 9). The outcome remains statistically significant meaning that we find an association between industries and type of fraud ($X^2(10)> = 46.151$, $p = 0.000$). This outcome shows that the industries in which the companies that are targeted operate significantly differ amongst types of fraud. CEO fraud mostly occurs in business services and industry companies whereas ghost invoices are mostly targeted towards business services and wholesale companies. Acquisition fraud is mostly targeted towards human health and social work activities companies and construction. As the first mentioned industries are the most targeted, we do see a trend of service based industries. As hypothesis 7 stated exactly that, we accept hypotheses 7.

Table 14:
*Cross tabulation of industry of defrauded company on types of fraud****

	CEO Fraud	Acquisition Fraud	Ghost Invoice
Industry	18	4	9
Construction	7	15	10
Wholesale, retail trade and repairs	17	13	20
Information and communication	12	2	3
Business services	23	14	28
Human health and social work activities	3	18	4
N	80	66	74

Chi-Square= 46.151; df=10, p=.000.
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

5.3.8 Size of defrauded company

When looking at the sizes of the companies we hypothesized that CEO fraudsters specifically target larger companies than ghost invoice senders, and ghost invoice senders larger companies than acquisition fraudsters. We ran a cross tabulation and find a significant difference amongst types of fraud (table 9). Meaning that there is an association between type of fraud and size of the defrauded company ($X^2(10)> = 172.028$, $p = 0.000$). This suggests that the sizes of the companies that are targeted significantly differ amongst types of fraud. Where in general very small companies are targets of acquisition fraud, small companies are targets of ghost invoices and medium sized companies are targets of CEO fraud. Where in acquisition fraud a downward trend is present from self-employed to very large companies,

such a trend cannot be found for CEO fraud and ghost invoices as there is more variation amongst sizes. Looking at these differences amongst types of fraud, we accept hypothesis 8.

Table 15:
*Cross tabulation of size of defrauded company on types of fraud****

	CEO Fraud	Acquisition Fraud	Ghost Invoice
Self-employed	0	44	26
Micro	5	43	36
Small	26	8	25
Medium	39	4	11
Large	18	1	0
Very large	12	0	1
N	100	100	99

Chi-Square= 172.028; df=10, p=.000.
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

5.3.9 Location of defrauded company

The final hypothesis, hypothesis 9, states that companies located in the western part of the Netherlands (Randstad) are more likely to be targets of fraud. When we first ran the cross tabulation for location of the company we see that even though there is an association, the assumption of expected count is not met. The location might be too specifically defined, as in for example Flevoland only two cases of fraud are present. Therefore, similar to what we did with industries we leave some provinces out of the analysis. When leaving the provinces out of the analysis that are only occasionally present in the dataset, seven provinces remain (table 10). The outcome remains statistically significant meaning that we find an association between location and type of fraud ($X^2(12) = 23.185$, $p = 0.026$). This outcome shows that the provinces in which the companies that are targeted are located significantly differ amongst types of fraud. CEO fraud (attempts) mostly occurred in Noord-Holland and Zuid-Holland, Acquisition fraud (attempts) mostly occurred in Noord-Holland and Gelderland, and Ghost Invoice (attempts) mostly occurred in Zuid-Holland and Gelderland.

Table 16:
*Cross tabulation of location of defrauded company on types of fraud**

	CEO Fraud	Acquisition Fraud	Ghost Invoice
Noord-Holland	30	18	18
Overijssel	5	7	4
Gelderland	4	16	20
Utrecht	9	4	6
Zuid-Holland	26	15	21
Noord-Brabant	17	14	15
Limburg	2	7	3
N	93	81	87

Chi-Square= 23.185; df=12, p=.026.
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

We could not do the cross tabulation with all twelve provinces of the Netherlands since they were too specific. Therefore, we ran the cross tabulation again, but now the location of the company is defined as either Randstad or Non-Randstad. The outcome is statistically significant meaning that we find an association between location (Randstad or Non-Randstad) and type of fraud ($X^2(2)> = 16.815$, $p = 0.000$). This outcome shows that the location of the companies that are targeted significantly differ amongst types of fraud. Where CEO fraud mostly occurs in the Randstad, acquisition fraud mostly occurs outside the Randstad and ghost invoices occur slightly more outside the Randstad. Looking at these results, we reject hypothesis 9. An overview of all hypotheses and their outcomes can be found in appendix 4.

Table 17:
*Cross tabulation of location of defrauded company (Randstad or not) on types of fraud****

	CEO Fraud	Acquisition Fraud	Ghost Invoice
Randstad	66	38	45
Non-Randstad	34	62	54
N	100	100	99

Chi-Square= 16.815; df=2, p=.000.
Note. * Significant: p < .05; ** Significant: p < .01; *** Significant: p < .001

5.4 Fraud and company characteristics and the effect on the amount asked

We have now shed light on the differences amongst the types of fraud with the use of bivariate analyses. From this section onwards, we advance to multivariate analyses and our first focus is on the financial aspect of fraud. As mentioned when discussing the descriptive statistics, we initially wanted to see what the effects of our variables were on the damages that companies suffered due to fraud. As we have too few cases in our dataset in which the fraud was successful, we decided to run the regression analyses with all cases, and use the amount asked by fraudsters instead of damages as a dependent variable. We should however keep in mind that the amounts that are mentioned in the following section are not actual damages that were suffered and thus could not be interpreted as such.

Looking back at the analytical framework, the relation that we are testing here are the possible effects of company and fraud characteristics on the amount asked by fraudsters. The dependent variable in this relationship is not normally distributed, the main reason for this is that the data includes cases of three different types of fraud. In order to test the relationship the variable amount asked by fraudsters was log transformed. In table 16, the results of the multiple regression on the dependent variable amount asked can be found. As we want to test the effects of the company and fraud characteristics but also the mediating effect of type of fraud the multiple regression consists of two models. Model one solely consist of the fraud and company characteristics, whereas model two additionally introduces the types of fraud.

The results from the multiple regression show some interesting outcomes. Looking at the company characteristic company size there seems to be a positive relationship with amount asked. In the first model, small, medium, large and very large company sizes all show a significant positive regression coefficient, indicating that company size has an effect on the amount a fraudster asks. In model two, however, the regression coefficients for small, large and very large sized companies is neither positive nor significant, whereas medium company

sizes still have a positive and significant regression coefficient. The fact that the effect of small, large and very large sized companies is gone and the regression coefficient of medium sized companies is significantly lower than in model 1 indicates that types of fraud play a mediating role in the relationship between company size and amount asked. Even though types of fraud influence the relationship the results still indicate that medium sized companies are asked 87% more than micro sized companies, with a standard deviation of 23% and controlling for the types of fraud.

In deciding what amount to ask companies fraudsters do not seem to take sector into account. None of the sectors have a significant regression coefficient in model 1 nor 2. As for industries there are some significant regression outcomes. In model 1, construction, wholesale and human health show significant negative regression coefficients. Once, the types of fraud are added in model 2, however, the coefficients are no longer significant. Instead, education and other service activities show significant negative regression coefficients. Indicating that companies in those industries are asked lower amounts than companies in business services. The results show that companies in education are asked 95% less and companies in other service activities 70% less, with standard deviations of 47% and 40% and controlling for the types of fraud.

Looking at the regression coefficients of the Dutch provinces we do not find many significant results. Only one of the provinces has a significant regression coefficient, and that is in model 2. In model 2, Overijssel has a positive significant regression coefficient. The coefficient from model 2 indicates that fraudsters, on average, ask %86 more of companies located in Overijssel than of companies located in Noord-Holland, with a standard error of 29% and controlling for the types of fraud.

When looking at the results of seasonality, the types of fraud again seem to have a mediating role in the relationship with amount asked. In model 1, we see that winter, summer and autumn have a positive and significant regression coefficient on amount asked. In model 2, the regression coefficients remain positive and significant but the strength of the effect is reduced. Whereas model 1 indicates that companies targeted in summer are asked 299% more than companies targeted in spring, model 2 indicates that companies targeted in summer are asked 64% more than companies targeted in spring. The same trend between model 1 and 2 can be seen for autumn and in to a lesser extent for winter.

As we know from the cross tabulations, ghost invoice senders ask significantly less than acquisition and CEO fraudsters, in addition ghost invoices are mainly send during the spring months. This explains why the significant regression coefficients are less strong in their effect once the types of fraud are introduced. As the results of seasonality are still significant in model 2 we do not speak of a mediating effect but off a mediating role of types of fraud, in the relationship between seasonality and amount asked by fraudsters.

Even though the results for the industries accommodation and food services, education, and other service activities and the province Overijssel are significant they could be questioned. As both these company characteristics have many categories, the frequency of cases within some of the categories is rather low. Taking into account that none of the other categories

within these variables have significant coefficients we state that fraudsters do not seem to take the location, sector, and industry of a company into account in deciding which amount to ask. They on the other hand do take the size of a company and the season into account.

Table 18:
Multiple regression analysis of company and fraud characteristics on amount asked by fraudster (N=226)

	Model 1 **Excluding types of fraud**		**Model 2** **Including types of fraud**	
	Multiple regression coefficients			
Variables	b	SE	b	SE
Company size				
Self-employed	-.02	.31	-.01	.17
Micro	Ref	Ref	Ref	Ref
Small	1.46***	.33	.31	.19
Medium	2.83***	.39	.87***	.23
Large	3.55***	.61	.57	.36
Very large	3.23**	.60	.50	.34
Sector				
Primary & Secondary	.59	.71	.06	.38
Tertiary	Ref	Ref	Ref	Ref
Quaternary	.73	.55	.09	.29
Industry				
Agriculture	-.61	.91	-68	.49
Industrial	-1.21	.78	-.39	.42
Construction	-1.79**	.76	-.25	.41
Wholesale	-.63*	.32	-.19	.17
Transport	-.21	.58	-.18	.31
Accommodation	.45	.61	.57*	.33
Information	-.22	.53	-.08	.28
Financial instit.	.23	.61	-.20	.32
Real estate	-.05	.70	.40	.37
Business services	Ref	Ref	Ref	Ref
Public services	x	x	x	x
Education	-1.41	.88	-.95**	.47
Human health	-1.03**	.48	.02	.26
Culture	-.38	.55	-.07	.29

Other services	-.62	.74	-.70*	.40
Company location				
Groningen	-.10	.63	-.27	.33
Friesland	.80	.74	.51	.40
Drenthe	-.51	.58	-.35	.31
Noord-Holland	Ref	Ref	Ref	Ref
Flevoland	x	x	x	x
Overijssel	.45	.54	.86**	.29
Gelderland	-.43	.38	-.03	.20
Utrecht	-.24	.45	-.09	.24
Zuid-Holland	-.10	.33	-.03	.18
Noord-Brabant	1.14	.97	.36	.51
Zeeland	-.23	.65	-.07	.35
Limburg	-.43	.73	-.03	.39
Seasonality				
Winter	.79**	.32	.74***	.18
Spring	Ref	Ref	Ref	Ref
Summer	2.99***	.30	.64**	.20
Autumn	1.51***	.37	.38*	.22
Types of fraud				
CEO fraud			4.38***	.25
Acquisition fraud			Ref	Ref
Ghost invoices			-.37**	.17
$\mathbf{R^2}$	R^2= .717		R^2= .921	

* Significant at the 0.1 level (2-tailed)
** Significant at the 0.05 level (2-tailed)
*** Significant at the 0.001 level (2-tailed)
Notes:
All categorical variables were recoded into dummy variables. Of every set of dummy variables one was left out of the regression. These variables are: tertiary, business services, noordholland, spring, acquisition fraud.

5.5 Fraud and company characteristics and the effect on successfulness

Our second focus is on the successfulness of fraud. Looking back at the analytical framework, the relation that we are testing here are the possible effects of company and fraud characteristics on the successfulness of fraud. In table 17, the results of the binary logistic regression on the dependent variable fraud successfulness can be found. As we want to test the effects of the company and fraud characteristics but also the mediating effect of type of

fraud the multiple regression consists of two models. Model one solely consist of the fraud and company characteristics, whereas model two additionally introduces the types of fraud. Small side not is that in order to reduce the amount of categories in the final binary logistic regression, the variable company location which originally included all twelve Dutch provinces was reduced to three categories. In the original analysis none of the provinces had any significant results hence our choice to reduce the number of categories. In addition, the variable industry was reduced to 8 categories instead of the original 15 categories. Industries that did not have significant output in the first analysis were combined into logical, but larger categories.

In table 17 we see that the company characteristic company size has no effect on fraud successfulness, in both models. The company characteristic sector, on the other hand, shows positive significant results for the category primary and secondary. Indicting that fraud attempts targeted at companies in the primary and secondary sector are, on average, 14.6 times more likely to be successful than those targeted at companies in the tertiary sector. The confidence interval, however, is very large indicating that the exact difference between the groups is hard to pinpoint but the relationship definitely is positive and significant.

As for industries, there are five categories that have a significant regression coefficients on fraud successfulness, in both models. With business services as the reference category we see that fraud attempts at companies active in industry and other primary & secondary industries are, on average, 0.03 times less likely to be successful. Same results, but the confidence interval is larger for other primary & secondary industries than for industrial companies.

Fraud attempts at companies active in real estate, education and health & social work are, on the other hand, more likely to be successful. With fraud attempts in the real estate industry being, on average, 9.5 times more likely. In education, on average, 54.5 times more likely and in health and social work, on average, 10.9 times more likely. All three confidence intervals are of such a size that we only confirm significance and direction but not the strength. The last company characteristic, company location, has no significant results.

Then on to the fraud characteristics, where seasonality has some significant results. Summer has a significant negative regression coefficient in both models and autumn has a significant negative regression coefficient in model 2. The results show that fraud attempts in summer are, on average, 0.1 times less likely to be successful. In addition fraud attempts in autumn are, on average, 0.2 times less likely to be successful. The confidence intervals of both seasons range from close to zero to around 1.3 times less likely.

The last fraud characteristic, amount asked shows significant and positive results for both the category €10.000 to €75.000 the category >€75000 only in model 1. This indicates that when fraudsters ask amounts within these categories they are more likely to be successful, 81.1 times more likely for the former category and 19.6 times more likely for the latter category. When, in model 2, we added the types of fraud into the regression only the category €10.000 -€75.000 remained significant, showing that fraud types might have a mediating role. This mediating effect however, cannot be confirmed because none of the regression coefficients of the fraud types are significant.

Table 19:
Binary logistic regression analysis of fraud and company characteristics on fraud successfulness (N=227)

	Model 1 **Excluding types of fraud**			**Model 2** **Including types of fraud**		
	Logistic regression coefficients					
Variables	β	OR	95% CI	β	OR	95% CI
Company Size						
Self-employed	.18	1.20	.23-6.15	.07	1.07	.21-5.57
Micro	Ref	Ref	Ref	Ref	Ref	Ref
Small	-.10	.91	.15-5.43	.11	1.11	.18-7.11
Medium	-.50	.61	.07-5.27	-.23	.79	.08-7.82
Large	-1.05	.35	.01-9.52	-.86	.42	.01-13.26
Very Large	-21.42	.00	.00	-21.26	.00	.00
Sector						
Primary and secondary	2.68**	14.53	1.07-197.29	2.68**	14.58	1.07-199.13
Tertiary	Ref	Ref	Ref	Ref	Ref	Ref
Quaternary	-1.75	.17	.01-3.17	-1.79	.17	.01-3.10
Industry						
Industrial	-3.65**	.03	.01-.72	-3.68**	.03	.01-.69
Real estate	2.22*	9.21	.84-101.23	2.25*	9.46	.85-105.67
Education	3.88*	48.25	.75-3088.79	4.00*	54.45	.84-3543.34
Health & Social work	2.43**	11.39	1.44-89.98	2.39**	10.87	1.38-85.89
Financial instit.	-.05	.95	.05-16.56	.07	1.08	.06-18.49
Business services	Ref	Ref	Ref	Ref	Ref	Ref
Other primary & secondary	-3.44*	.03	.01-1.50	-3.57*	.03	.01-1.03
Other tertiary	.27	1.31	.31-5.49	.19	1.21	.28-5.16
Company location						
North-East	.11	1.12	.29-4.27	.02	1.02	.25-4.20
West-Randstad	Ref	Ref	Ref	Ref	Ref	Ref
South	-.10	.91	.22-3.75	-.15	.86	.21-3.57
Seasonality						
Winter	-1.21	.30	.05-1.84	-1.49	.23	.03-1.59
Spring	Ref	Ref	Ref	Ref	Ref	Ref
Summer	-2.51**	.08	.01-.68	-2.69**	.07	.01-.62

Autumn	-1.58	.21	.03-1.64	-1.88*	.15	.02-1.31
Amount asked						
0-200	Ref	Ref	Ref	Ref	Ref	Ref
200-400	.03	1.03	.12-8.79	-.38	.69	.07-7.07
400-10000	1.36	3.89	.62-24.50	1.15	3.16	.49-20.48
10000-75000	4.46***	86.43	7.13-1047.21	4.40**	81.10	1.57-4191.64
>75000	3.04**	20.96	1.23-357.48	2.98	19.61	.25-1538.30
Type of fraud						
CEO Fraud				-.69	.50	.01-23.26
Acquisition Fraud				Ref	Ref	Ref
Ghost Invoices				-.78	.46	.08-2.81

* Significant at the 0.1 level (2-tailed)
** Significant at the 0.05 level (2-tailed)
*** Significant at the 0.001 level (2-tailed)
Notes: Dependent variable is successfulness of fraud (0=unsuccessful, 1=successful).
Abbreviations: ref = reference category; OR – odds ratio; CI – confidence interval; P = probability.

6. Discussion and Conclusion

In this section the results from the previous chapter will be analysed and discussed in relation to the posed theories. This will lead to a conclusion and the answering of the research question. Lastly, limitations, and some recommendations for future research are presented.

6.1 Discussion

The aim of this study was to shed light on fraud in which companies are targeted. Looking at the data that we gathered, an interesting set of notifications resulted in a solid dataset. The first striking outcome of our study is that only eight percent of the fraud attempts was successful. This gives rise to the question if this percentage is a realistic representation of the fraud attempts that are successful. A fraud is successful when the fraudster receives money from his target, irrespective of whether the target eventually finds out that he was defrauded. If a victim of fraud does not know that he was defrauded, he cannot report it to the FHD. In addition to the uncovering of fraud attempts, a company might also see no reason to report fraud out of embarrassment for example (Zwetsloot, 2017). A company might not want others to know that they were defrauded or they might have employees in-house that focus on fraud. These arguments make it likely that our rate of success is not representative for the actual success rate amongst fraud attempts.

Looking at the types of fraud, we could not confirm that there were differences amongst them with regards to the success rate. When we looked at scalability in combination with the success rate and average earnings we did find interesting new perspectives. Whereas the success rates are only about one percent apart the scalability of the fraud types are distinct. This was also reflected in the crime script analysis. Looking at the small differences in success rate one would say that ghost invoices are the most efficient type of fraud as they require the

lowest effort. The average earnings however show that, when successful, fraudsters can gain two hundred times as much with CEO fraud than with ghost invoices.

This low success rate does not mean that fraudsters are not trying to achieve high success rates. According to the rational choice theory, fraudster try to achieve high success and low effort. The results show that seasonality is something that fraudsters take into account in timing their fraud attempts. Our results show that most CEO fraud happens during summer, most ghost invoices are send during spring and acquisition fraud is at a peak during winter and spring. This suggests that fraudsters estimate that companies are more likely to fall for a certain type of fraud during specific seasons. It might be wise if companies make their employees aware of the types of fraud that could potentially be attempted in certain seasons.

The same trend is present in the results on the amount asked by the fraudsters. CEO fraudsters ask substantially more than acquisition fraudsters, and ghost invoice senders on their turn ask less than acquisition fraudsters. This seems to be a well estimated choice that fraudsters make in assessing the chance of success and what amount to ask. This outcome makes CEO very dangerous as the amounts that are asked are hundreds of thousands of euros. Acquisition fraud and ghost invoices however are tricky as well. If companies do not have specific systems in place they could end up paying dozens of ghost invoices.

The present study also looked at information about the identity or location of fraudsters, based on the bank details that were provided in the fraud (attempt). Looking at acquisition fraud and ghost invoices fraudsters seem to be located in the Netherlands, whereas CEO fraudsters are located outside the Netherlands. With all three types of fraud, the bank details mostly refer to a company. What makes it hard to draw conclusions from our output is that fraudsters are known use money mules or shell companies. This makes it very hard to say anything about the identity and location of fraudsters (Grijpink, 2006).

Early in the analyses we showed that the Dutch economic landscape of 2016 is very similar to the fraud notifications that the FHD received in 2016. When we look at the differences amongst types of fraud we see that, apart from sector, all company characteristics are different amongst fraud types. Hence, indicating that the Dutch economic landscape of 2016 does not necessarily play a role in the distribution of fraud amongst Dutch companies. The differences amongst types of fraud show that it is very likely that company characteristics play a role in which type of fraud a company is likely to encounter.

As not much information is known about the fraudsters it is much more interesting to study the victims. Therefore, the present study also analysed characteristics of the companies that were targeted. The results showed no difference amongst the fraud types, amongst all fraud types fraudster seem to prefer to target companies that operate in the tertiary sector. Whereas our analysis also shows, that the chance of success of a fraud attempt is considerably larger if attempted against a company active in the primary or secondary sector.

Something different seemed to be true for industries. Where CEO fraudsters and ghost invoice senders mostly target companies operating in business services, acquisition fraudsters target human health and social work activities. These industries are largely service based industries, which confirmed our expectations. It does seem that fraudsters distinguish between these

tertiary industries depending on the type of fraud they attempt. This is interesting as for example the crime script for ghost invoices shows that fraudsters send invoices to thousands of companies. The routine activity theory might help in answering this question. If a fraudster begins with sending ghost invoices by using certain ways of searching potential companies it might become a routine to select companies that way. Hence, without specifically selecting companies in a certain industry a fraudster unknowingly operates in certain industry.

Within these sectors and industries companies of all sizes operate. What is interesting about the size of a company is whether fraudsters take it into account in choosing their targets and setting the amounts to ask. We expected CEO fraudsters to specifically target larger companies than acquisition fraudsters and ghost invoice senders and this was confirmed by our results. Results show that CEO fraudsters seem to prefer medium sized companies (50-250 employees), acquisition fraudsters prefer self-employed people and ghost invoice senders micro companies (2-10 employees). As mentioned in the introduction, smaller companies often do not have the resources to keep up with fraudsters and when defrauded they are more likely to experience financial distress. These outcomes are bad news for the self-employed and small business owners. Large companies invest in making their employees more aware of the dangers of fraud but small companies and especially the self-employed are less likely to do so. Making them the new, very vulnerable targets of fraudsters (Zwetsloot, 2017).

Rational choice predicts that fraudsters weigh the benefits against the costs and want low effort and high gains. We know by now that the highest gain can be achieved by CEO fraud. However, if the chance of CEO fraud success is significantly lower with relatively small companies, as opposed to larger companies, fraudsters are more likely to attempt CEO fraud with larger companies. The same goes for acquisition fraud and ghost invoices, as large companies might be more able to detect fraudulent invoices and less open for acquisition, than self-employed and smaller companies. Hence, smaller companies could direct their efforts towards protecting themselves against ghost invoices and acquisition fraud whereas larger companies could focus on CEO fraud.

The last company characteristic that was analysed is location. Our results show that Noord-Holland, Zuid-Holland and Gelderland are the provinces in which most of the targeted companies are located. Looking at the revenue per province we see that the three provinces in which most target companies are located are also one of the most economically active regions. As we know that fraudster find their victims on the internet these results are no surprise and proves that location does not make a company more or less vulnerable for fraud.

Looking at the crime scripts, we see that they are very distinct of one another. With CEO fraud the most interesting aspect is that the fraudsters asks the employee to disregard any protocols and wire the money. This should be a big red flag for employees but in practice CEO fraud attempts do often succeed. This raises the question whether it is normal that executives asks employees to do tasks without following protocol. The same goes for ghost invoices, you would expect companies to have systems in place with which they can verify invoices. Just like CEO fraud, ghost invoices do get paid and thus the fraud succeeds.

Of course, when a company is in a very hectic and busy phase it is more important that things get done than the way they get done. This might be something of which fraudsters profit as making mistakes is human. This brings us to probably the most effective way to prevent fraud, letting machines do the work. If all payments that a company makes are verified by some sort of system a lot of fraud attempts will be prevented. The focus should be on providing fraudsters with barriers that make the chances of success very slim. If that is the case than fraudsters would no longer think that the benefits outweigh the costs and that the efforts are much higher than their potential gain. In a perfect scenario, barriers provide fraud prevention on the short term and drastically reduces the fraud attempts on the long term.

6.2 Conclusion

Now, looking back at the research question we posed:

How do acquisition, invoice and CEO fraud differ amongst each other when looking at fraud and company characteristics? To what extent do fraud and company characteristics have an effect on financial damage and fraud successfulness? Can these insights, when combined with crime scripts, lead to preventive measures?

According to our results, there are many differences between the three types of fraud. Acquisition fraud is more likely to be attempted in winter and against self-employed and micro companies. Ghost invoices are more likely to be attempted in spring and against micro and small sized companies. CEO fraud is more likely to be attempted in summer and against small and medium sized companies.

The amount asked is largely dependent on the fraud that is attempted. However, larger companies are more likely to be targets of CEO fraud and are hence asked higher amounts. Meaning that companies that are targets of CEO fraud have the highest risk with regards to financial damage, followed by acquisition fraud and ghost invoices. Whereas most attempts are directed towards the tertiary sector, the chance of success is higher in the primary and secondary sector. This means that the primary and secondary sector are rather vulnerable.

The crime scripts show that there are a certain amount of steps a fraudster takes in committing any of the three types of fraud. The self-employed should be aware of the dangers of acquisition fraud, especially in winter, and never accept or agree to anything without checking the details. Small companies should be aware of ghost invoices, which are mostly send in spring, and make their financial department aware of the procedures in checking and paying invoices. Larger companies should be more aware of CEO fraud in summer and look for irregularities in email traffic with the CEO. With these insights, and knowing the modus operandi of fraudsters, companies can focus more on their vulnerabilities.

6.2.1 Limitations and future research

In this section the limitations of the present study will be discussed, and recommendations are given for further research. The first limitation, is that no actual damages were analyzed. The aim was to see whether company and fraud characteristics played a role in the damage that companies suffered. Due to the low rate of successfulness the aim shifted towards looking how fraudsters set the amounts they ask.

For future research it would interesting to specifically collect data in which the fraud attempt was successful. Because a limitation of the present study is that we have no information on why fraud attempts were prevented. Is it because those companies invest in awareness amongst their employees or is there another reason. It would be very interesting to do interviews with companies in which the fraud was successful and in which the fraud was unsuccessful. These can then be compared which could possibly result in interesting new insights.

In addition, it is very difficult to draw conclusions about fraud as we do not have data over several years, so we cannot see whether there is a trend. Our results might have been different if we would have collected data on fraud notifications in another year. Hence, our recommendation for future research is to collect data on fraud over several years and then comparing the years to see whether trends can be found. If a trend for example is that fraudsters seem to shift more towards a certain industry or company size, barriers can be put in place to protect these companies.

Lastly, this research has limited information on the fraudster that attempted the fraud. Fraudsters are a group of people that are very clever in hiding behind company names and other people. We can only make assumptions in what the motives of fraudsters are in for example attempting fraud in a specific season.

6.2.2 Recommendations

The present study use data collected by the Fraudehelpdesk (FHD). With the outcomes, institutions, like the FHD, can shift their attention towards specific groups of companies and their vulnerabilities. We now know that company characteristics and seasonality play a role in the vulnerabilities of companies, these aspects in particular can help the FHD in their battle against fraud. Our recommendation is that the FHD uses the outcomes of this research to warn and alert companies with regards to their vulnerabilities. In addition, the FHD could focus their marketing strategy towards the seasonality of fraud. In conclusion, this research has shown that fraud is a multidisciplinary concept and every type of fraud needs to be dealt with in a different way. The modus operandi of all types are very straightforward which makes it relatively simple to put preventive measures in place and increase awareness.

References

Abell, P. (1991). Rational choice theory. *Aldershot: Elgar.*

Accura (2017). The Fraud Ultimatum. Retrieved on the 17th of September 2017 from: https://www.vocalink.com/downloads-and-media/reports/the-fraud-ultimatum/

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour. *Prentice-Hall*, 1-278.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Ajzen, I. (2006). Constructing a theory of planned behavior questionnaire. 1-12.

Andresen, M. A., & Malleson, N. (2013). Crime seasonality and its variations across space. *Applied Geography*, *43*, 25-35.

Beauregard, E., Proulx, J., Rossmo, K., Leclerc, B. & Allaire, J.-F. (2007), Script analysis of the hunting process of serial sex offenders. *Criminal Justice and Behavior,* 34(8), 1069-1084.

Bloem, B. & Harteveld, A. (2012). Horizontale Fraude: Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2012. 1-186*.*

Bloem, B. (2013). Horizontale fraude in kaart. *Het Tijdschrift voor de Politie, 75(7), 30-34.*

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review, 15*(6), 738-743.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime prevention studies*, *3*, 151-196.

Cornish, D. B., & Clarke, R. V. (2008). The rational choice perspective. *Environmental criminology and crime analysis*, *21*, 21-47.

Cullen, F., Eck, J., & Lowenkamp, C. (2002). Environmental corrections: A new paradigm for effective supervision. *Federal Probation*, 66(2), 28–37

Dorminey, J. A., Fleming, S. A., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in accounting education,* 27(2), 555-579*.*

Duffield, G., & Grabosky, P. (2001). The Psychology of Fraud. *Australian Institute of Criminology*, 199, 1-6.

Duffield, G., & Grabosky, P. (2001). Red Flags of Fraud. *Australian Institute of Criminology,* 200, 1-6.

European Federation of Accountants (2005). How SMEs can reduce the risk of fraud. *European Federation of Accountants,* 1-28.

Falk, G. J. (1952). The influence of the seasons on the crime rate. *The Journal of Criminal Law, Criminology, and Police Science*, *43*(2), 199-213.

Friedman, M. (1953). Essays in Positive Economics. *University of Chicago Press*.

Fraudehelpdesk (2017). Handboek Fraudevormen. Retreived via email on the 13th of September 2017.

Grijpink, J. H. A. M. (2006). Identiteitsfraude en overheid. *Justitiële verkenningen*, *4*(7), 3.

Hancock, G. & Laycock, G. (2010). Organised crime and crime scripts: prospects for disruption. *Situational prevention of organised crimes*, 172-192, New York: Taylor & Francis US.

Hipp, J. R., Curran, P. J., Bollen, K. A., & Bauer, D. J. (2004). Crimes of opportunity or crimes of emotion? Testing two explanations of seasonal change in crime. *Social Forces*, *82*(4), 1333-1372.

Huisman, K., van de Bunt, H. G., Eeren, H. V., Kwaspen, I. J. J., & Boer, I. M. (2009). Misleidende handelspraktijken: een onderzoek naar de aard, achtergronden en aanpak van acquisitiefraude in Nederland.

Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596-614.

Junger, M., Montoya, L., Hartel, P., & Karemaker, M. (2013). Modus Operandi onderzoek naar door Informatie en Communicatie Technologie (ICT) gefaciliteerde criminaliteit.

Lambregts, B. (2008). Geographies of knowledge formation in mega-city regions: some evidence from the Dutch Randstad. *Regional Studies*, *42*(8), 1173-1186.

de Lange, R. (2017). Privacywaakhond ligt dwars bij nieuw wapen tegen fraude. Financieel Dagblad, 09-10-2017, 1.

Lauritsen, J. L., & White, N. (2014). *Seasonal Patterns in Criminal Victimization Trends*. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Leclerc, B., Wortley, R. & Smallbone, S. (2011), Getting into the script of adult child sex offenders and mapping out situational prevention measures. *Journal of Research in Crime and Delinquency, 48(2),* 209-237.

LeClerc, B., & Wortley, R. (2013). *Cognition and crime: Offender decision making and script analyses*. Routledge.

Levy, M., & Powell, P. (2003). Exploring SME internet adoption: towards a contingent model. *Electronic markets*, *13*(2), 173-181.

Lohrke, F. T., Franklin, G. M., & Frownfelter-Lohrke, C. (2006). The Internet as an information conduit: A transaction cost analysis model of US SME Internet use. *International Small Business Journal*, *24*(2), 159-178.

Schalke & Partners (2014). Fraude kost Nederland jaarlijks 30 miljard. Aanpak loont. Retrieved on the 22nd of November from: http://www.schalke.nl/pdf/FRAUDE-totaaloverzicht%202014.pdf

Statistics Netherlands (2015). De staat van het mkb. *Panteia & ministerie van Economische Zaken*, 1 – 66.

Statistics Netherlands (2017). Geregistreerde criminaliteit. Retrieved on the 17th of September 2017 from: https://www.cbs.nl/nl-nl/cijfers#theme=veiligheid-en-recht

Statistics Netherlands. (2018). Statistics Netherlands: Bedrijven, Bedrijfstak [Dataset]. Retrieved March 27, 2018, from: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81589NED/table?ts=1525168196752

Statistics Netherlands. (2018). Statistics Netherlands: Bedrijfsleven; omzet, bedrijfstak (SBI 2008), regio [Dataset]. Retrieved February 21, 2018, from: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83796NED/table?ts=1525168504418

Van Geldrop, A., & De Vries, T. (2015). Fraude loont… nog steeds. *Stichting Toekomstbeeld der Techniek.*

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Zweighaft, D. (2017). Business email compromise and executive impersonation: are financial institutions exposed? *Journal of Investment Compliance*, *18*(1), 1-7.

Zwetsloot, J. (2017). Ondernemers steeds vaker opgelicht, vooral kleine zeflstandigen zijn doelwit. Retrieved on the 21st of March from: https://www.volkskrant.nl/economie/ondernemers-steeds-vaker-opgelicht-vooral-kleine-zelfstandigen-zijn-doelwit~a4466023/

Appendix

Appendix 1: Coding Scheme

Table 20: Coding Scheme

No.	Name	Label	Possibilities
1	Date	Date of entry by encoder	
2	Casenumber	12-digit number with which FHD indicates a unique case	
3	Status	Status of the report	1. Unsolved 2. Updated 3. Waiting for reporter 4. Incomplete file 5. Solved 6. Automatically answered 7. Send to coordinator 8. Rejected by coordinator 9. Handled 10. Accepted by coordinator 11. Handled in dossier 12. Call reporter 13. Send to legal department 14. Is being handled 15. Send to participantadmin
4	Permission	Permission for further research/contact	1. Yes 2. No 99. Unknown
5	TypeofFraud	The type of fraud reported	1. CEO Fraud 2. Identity Theft 3. Acquisition Fraud 4. Ghost Invoice
6	DateofFraud	The date the fraud was (tried to be) committed	
7	DateofFraudNoticed	The date the (intended) fraud was noticed	
8	How_noticed	How was the (intended) fraud noticed?	Text
9	Approach_type	The type of approach used to commit the fraud	1. Email 2. Fax 3. Online 4. Personal 5. Post 6. SMS 7. by Telephone 8. Whatsapp 9. No approach 10. Other 99. Unknown
10	Approach_comment		Text

11	Use_of_internet	Was the internet used in (trying to) commit the fraud?	1. Yes 2. No 99. Unknown
12	Internetcomment		Text
13	Fraud_Prevented	Was the fraud prevented, was it a failed attempt?	1. Yes 2. No 99. Unknown
14	Paid	Was the fraudster paid?	1. Yes 2. No 99. Unknown
15	Who_duped	Who is duped?	1. Company 2. Customer 3. Not applicable 99. Unknown
16	AmountAsked	What was the amount charged/asked by the fraudster?	
17	Damage	Was there damage due to the fraud?	4. Yes, financial damage 5. Yes, image damage 6. No 99. Unknown
18	Fraudster_identity	Is the identity of the fraudster known?	1. Yes, the name of the person(s) 2. Yes, the name of the company 3. No 99. Unknown
19	Fraudster_origin	Where is the fraudster (operating) from?	1. the Netherlands 2. Europe (except NL) 3. Africa 4. Asia 5. America 6. Australia 99. Unknown
20	Fraudster_origin_comment		
21	Industry	Industry the Defrauded SME is active in. Categorized with the use of SBI-2008 code of Statistics Netherlands	1. Agriculture, forestry and fishing (A) 2. Industry (B/C/D/E) 3. Construction (F) 4. Wholesale and retail trade, repairs (G) 5. Transport and storage (H) 6. Accommodation and food service (I) 7. Information and Communication (J) 8. Financial institutions (K) 9. Renting, buying and selling of real estate (L) 10. Business Services (M/N) 11. Public services (O) 12. Education (P)

			13. Human health and social work activities (Q) 14. Culture, sports and recreation (R) 15. Other service activities (S)
22	Sector	Industry the Defrauded SME is active in. Broadly Categorized	1. Primary and Secondary Sector 2. Tertiary Sector 3. Quaternary Sector
23	Industry/Sector_comment		Text
24	Size_category	What is the size of the SME in terms of employees?	1. 1 (self-employed) 2. 2-10 (micro) 3. 11-50 (small) 4. 51-250 (medium) 5. 250-1000 (large) 6. 1000+ (very large 99. Unknown
25	Size_number	What is the size of the SME in terms of FTE?	
26	Location_city	What is the (main) location of the defrauded company? (city)	
27	Location_province	What is the (main) location of the defrauded company?	1. Groningen 2. Friesland 3. Drenthe 4. Noord-Holland 5. Flevoland 6. Overijssel 7. Gelderland 8. Utrecht 9. Zuid-Holland 10. Noord-Brabant 11. Zeeland 12. Limburg 99. Unknown
28	Investigation	Was this case investigated / linked to other cases?	1. Yes 2. No
29	Investigation_name	Name of Investigation (fictional)	
30	BindingFactor	What was the binding factor in the investigation?	1. Type of fraud 2. Modus Operandi 3. Establishment of agreement 4. Involved person 5. Involved entity 6. Not applicable 99. Unknown
31	CasesInvestigation	Number of cases collected in the investigation	

Appendix 2: Scenes and Actions – Crime script framework

Table 21: Crime Script Framework (LeClerc & Wortley, 2013)

Script scenes	**Script actions**
Preparation	
Entry	
Precondition	
Instrumental precondition	
Instrumental initiation	
Instrumental actualization	
Doing	
Post-condition	
Exit	

Appendix 3: Histograms

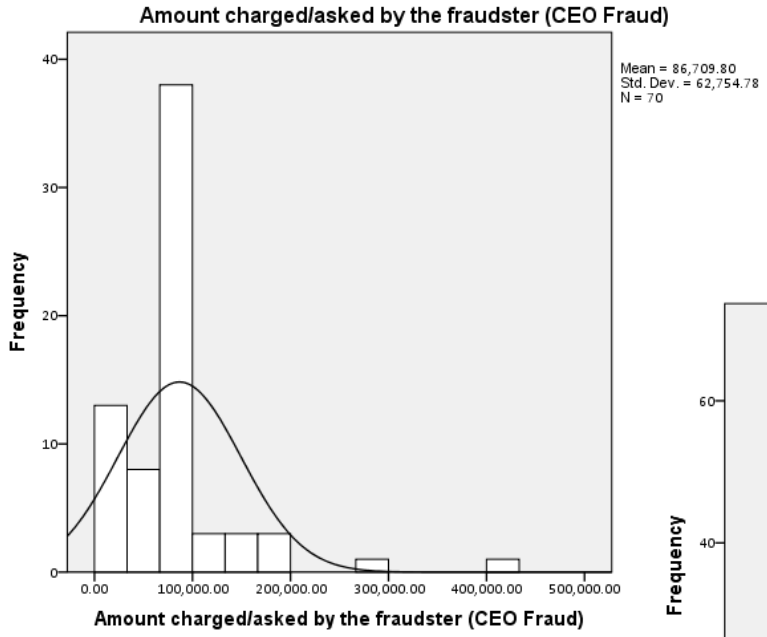

Figure 6: Histogram amount asked by fraudster for CEO Fraud

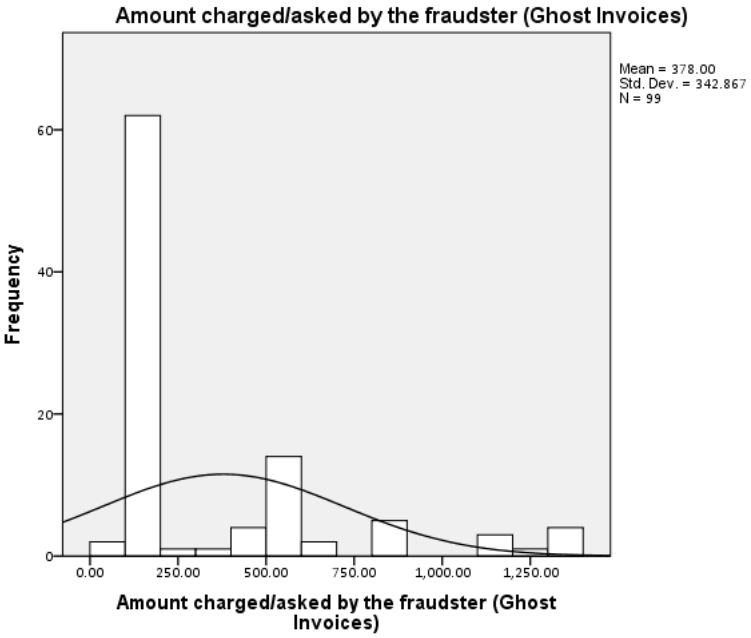

Figure 7: Histogram amount asked by fraudster for Ghost Invoices

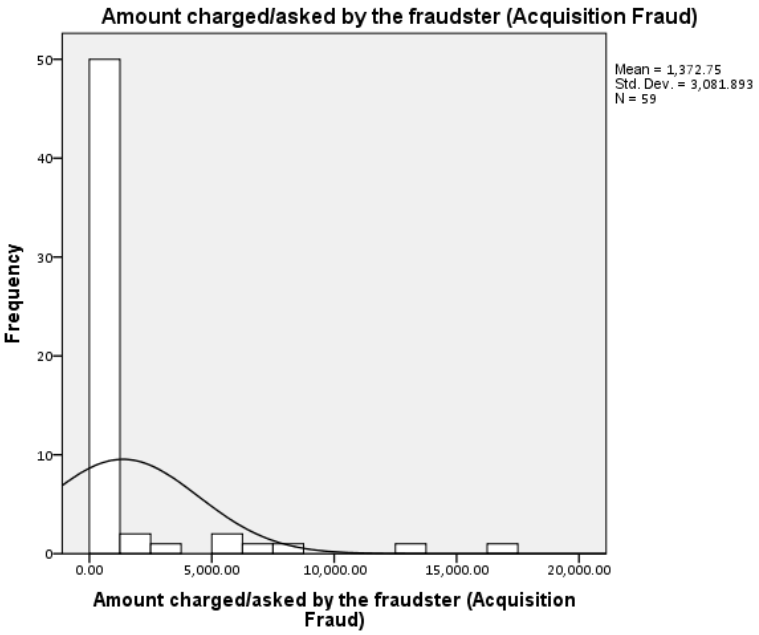

Figure 8: Histogram amount asked by fraudster for Acquisition Fraud

Appendix 4: Overview of hypotheses and outcomes

Table 22:
Overview of accepted and rejected hypotheses

Hypotheses	Rejected / Accepted
Hypothesis 1: The success rate of fraud attempts differs amongst types of fraud. CEO fraudsters experience the highest rate of success and ghost invoice senders the lowest rate of success.	**Rejected**
Hypothesis 2: Fraudsters are more likely to try and defraud a company during the summer than during other seasons.	**Rejected**
Hypothesis 3: The financial damage differs amongst types of fraud. It is the lowest when it concerns ghost invoices, a bit more when it concerns acquisition fraud and the highest when it concerns CEO fraud.	**Accepted**
Hypothesis 4: Whether or not aspects are known about the identity of the fraudster does not differ amongst types of fraud as in most cases only the name of a (front) company is known.	**Accepted**
Hypothesis 5: The location of the fraudsters differ amongst types of fraud. Fraudsters are mostly located in the Netherlands with regards to ghost invoices and acquisition fraud, and outside the Netherlands with regards to CEO fraud.	**Accepted**
Hypothesis 6: Companies operating in the tertiary sector are more likely to be targets of fraud, than companies operating in the primary, secondary and quaternary sector.	**Accepted**
Hypothesis 7: Companies operating in more service-based industries are more likely to be targets of fraud, than companies operating in other industries.	**Accepted**
Hypothesis 8: Large companies are more likely to be targets of CEO fraud, whereas smaller companies are more likely to be targets of acquisition and invoice fraud.	**Accepted**
Hypothesis 9: Companies located in the western part of the Netherlands (Randstad) are more likely to be targets of fraud.	**Rejected**