Crime Science

RESEARCH

Open Access

Fraud against businesses both online and offline: crime scripts, business characteristics, efforts, and benefits

Marianne Junger[1*], Victoria Wang[2] and Marleen Schlömer[3]

Abstract

This study analyses 300 cases of fraudulent activities against Dutch businesses, 100 from each of the following three categories: CEO-fraud, fraudulent contract, and ghost invoice. We examine crime scripts, key characteristics of targeted businesses, and the relationship between input criminal effort and output financial benefit. Results indicate that whilst all CEO-frauds are conducted online, most of the fraudulent contracts and ghost invoices are undertaken via offline means. Both Routine Activity Theory and Rational Choice Model are evidenced-fraudsters clearly take the business size and seasonality into account, and the input criminal effort and output criminal benefit are positively correlated. Having vigilant employees is evidenced as the most effective way of fraud prevention, both online and offline.

Keywords: CEO fraud, Fraudulent contract, Ghost invoice, Routine Activity Theory, Rational Choice Model, Preventative measures

Fraud is a broad concept, and accordingly, it has been studied by various disciplines (e.g., Piquero and Benson 2004; Simpson 2010). Academically, it could be understood as “an uncommon, well-considered, imperceptibly concealed, time-evolving and often carefully organized crime which appears in many types and forms” (Van Vlasselaer et al. 2015: 39–40). In practice, the ‘fraud’ label covers a broad range of activities (for a summary, see: Levi and Burrows 2008). Fraud can target private individuals, businesses or governmental organisations and is to leads to relatively high costs. Although the primary costs of fraud are obvious, potential secondary costs may be equally harmful: diminished faith in an organization, loss of stakeholders’ trust and market valuation, and erosion of public morality (PWC 2018).

Interestingly, incidence levels for fraud do not follow the same trend as for other crimes. Scholars seem to agree that, in general, crime rates are decreasing in the Western world (Farrell 2013). In contrast, in recent years, fraud statistics have shown alarming increases. This is especially significant in the US (NCJRS 2017), the UK (Financial Intelligence Group. 2017), and the Netherlands (Statistics Netherlands 2018b). In the Netherlands, for instance, between 2005 and 2017, ‘deception’ increased by a factor of 2.3, ‘forgery’ by a factor 2.4, ‘extortion’ by a factor of 1.8, and ‘hacking a computer system’ by a factor of 3.9 (Statistics Netherlands 2018b).

This sharp rise of fraud is generally attributed to the fact that much fraudulent activity is now cyber-related, especially cyber-enabled.[1] In 2011, for instance, 41% of all

*Correspondence: m.junger@utwente.nl
[1] Department of Industrial Engineering and Business Information Systems, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands
Full list of author information is available at the end of the article

[1] Many authors and organisations differentiate between cyber-enabled crimes and cyber-dependent crimes. Cyber-enabled crimes are traditional crimes but executed by use of computers, computer networks or other forms of information communications technology. Cyber-dependent crimes are usually defined as crimes that can only be committed using computers, computer networks or other forms of information communication technology (ICT). Example are a DDoS attacks of hacking McGuire and Dowling (2013) Cyber crime: A review of the evidence. London, UK: Home Office.

fraudulent activities in the Netherlands was cyber-related (Montoya et al. 2013). Going online makes fraudsters much more flexible and permits internationalisation of crime (Levi 2008).

Data on fraud are scarce. This has seriously limited the number of studies on the subject (National Academies of Sciences 2018: 44; Piquero and Benson 2004; Simpson 2010). Much of the research on fraud offenders has been qualitative data and case studies often based on interviews with small samples, without including control groups of non-criminals or 'street-crime' criminals (Simpson 2010). There is also very limited information on the extent of victimization of fraud and few instruments exist that have been updated to include online fraud (Deevy et al. 2012; Deevy and Beals 2013). Many fraud studies did not quantify the measurement of concepts; many of them were hard to operationalize and measure independent of each other (Schuchter and Levi 2013). This state of affairs led Piquero and Benson (2004) to conclude that a 'statistical valid picture of white-collar criminals is hard to come by' (Piquero and Benson 2004: 154).

The present study will dive deeper in three specific forms of fraud that target businesses, namely: CEO-fraud,[2] ghost invoices, fraudulent contracts. It aims to describe, for each type of fraud, the fraud scripts, the characteristics of the victimized businesses, and the characteristics of the fraud. Furthermore, it will present data on how the fraud was prevented. We believe we are presenting unique data, as specific information on fraud victimization of businesses is usually kept confidential. Also, to the best of our knowledge, this study is the first to present quantitative data on CEO fraud. We begin, below, by presenting a broad approach to theories of fraud. Thereafter, we present the Routine Activity Theory and the Rational Choice Model of Crime that will be used as guiding theoretical frameworks.

Background

Theories of fraud

The causal factors of fraud have originally been described in a model called the "Fraud Triangle" (Cressey 1965) that focussed on the white-collar offender: three elements need to be present for fraud to occur.

1) Motive (or pressure). Violators of trust often have a financial problem and perceive this problem to be 'non-shareable' (Cressey 1965). Several authors proposed a broader range of motivators, besides money, such as ideology, coercion or 'Ego (entitlement)' (Dorminey et al. 2012).
2) Opportunity. Violators are aware that their problem can be secretly resolved by the violation of the position of financial trust, the situation that enables fraud to occur (often when internal controls are weak or non-existent) (Cressey 1965). All researchers seem to regard opportunity as an important—although not sufficient—condition for fraud to occur (Schuchter and Levi 2013; Dorminey et al. 2012; Murphy et al. 2011).
3) Rationalization. This refers to the mindset of the fraudster that justifies the execution of a fraud. In later publications, Cressey—in line with Sutherland's social learning theory (Sutherland and Cressey 1974) argued that the rationalization process, is, sufficient to commit fraud (Cressey 1964).
   Other concepts have also been noted as well in the fraud literature as causal factors of involvement in fraud.
4) Company culture. According to Schuchter and Levi (2013), the pressure within the company is the most important motivator for fraud in contrast with motivators within the fraudster him/herself or his/her personal situation (Schuchter and Levi 2013: 8–9).
5) Capability. Wolfe and Hermanson (2004) noted that fraudsters need to have the capabilities to turn an opportunity into a real fraud.
6) Detection. Simpson et al. (2014) noted, in a literature review, that the fear of detection is an important contributor to fraud, the likelihood of detection should deter fraud.

For the present study, with a focus on victimized businesses, theories of crime science, namely the Rational Choice Model of crime and Routine Activity Theory are used. Routine Activity theory comprises the opportunity structure of a company and the capabilities of fraudsters as described above; the Rational Choice Model includes the likelihood of detection. Motives, rationalisation by fraudsters and company culture are beyond the scope of the present study. Below we describe how these approaches can be used in the context of businesses. Other elements could not be assessed in the present study.

Theoretical approach in the present study

Routine Activity Theory (RAT)

RAT was developed by Cohen and Felson Cohen and Felson (1979) and later developed by Felson (1995). Brunet

[2] *CEO Fraud* happens when cybercriminals impersonate executives and trick other employees into executing unauthorized payments via wire transfers. There is no legal definition of CEO-fraud, accordingly it refers to what practitioner have agreed to as what it means. Readers can find additional information on: https://www.actionfraud.police.uk/alert/action-fraud-warning-after-serious-rise-in-ceo-fraud.

(2002) provides a comprehensive review. In short, RAT stresses the importance of exposure and vulnerabilities of targets to potential offenders in the context of decreased guardianship (Tilley and Sidebottom 2015). The amount of time individuals spent outdoors, and the activities performed at night and during weekends are strong correlates of their likelihood of victimization of a wide variety of crime types, including property and violent crime (for a review, see also Tilley and Sidebottom (2015)), as well as fraud (Holtfreter et al. 2008). Besides more theoretical oriented studies, the importance of opportunities for fraud has been emphasized by various scholars (Benson et al. 2009; Button et al. 2009).

Building on previous studies that operationalised exposure and routine activities for businesses, we propose that the following business characteristics could be conceptualised as opportunities and to the routine activities of businesses: (1) business service orientation, (2) business size, (3) business location and (4) seasonality.

1) Business service orientation. The service industry's focus is directed to maintaining customer contact and providing services in a customer-friendly way. The focus of a product-based business is, in contrast, to provide the product that is ordered by the customer (Lohrke et al. 2006). It seems plausible that service-based businesses, having many customer contacts, are, therefore, more vulnerable to fraud. The present study will investigate whether fraud type is related to the economic sector and the service orientation of a firm.
2) Business size. In terms of types of fraud, business size as a factor might relate to vulnerability. Several studies reported different trends, but generally, larger businesses usually suffer larger losses from fraud (BCC 2008; Finnerty et al. 2018). In line with the RAT, several explanations may be offered. First, a large business is probably better known by the public, including offenders, and maybe more visible online, which increased its online exposure. Second, large businesses usually deal with bigger sums of money, and as a result, become more attractive targets. PWC (Coopers 2014), for example, found that large businesses are at more risk of cyber-related crimes. Third, large businesses often do business across national borders, providing fraudsters with opportunities to defraud businesses in countries with characteristics that are conducive to crime, e.g., a less solid legislative framework (Zweighaft 2017). Fourth, large businesses usually have more complicated organisational structures. Many have different chains of command, leading to a targeted employee experiencing greater difficulties in identifying requests from a fraudster (Zweighaft 2017). Fifth, larger businesses may be targeted by different types of fraud in contrast to smaller businesses (Verizon Risk Team. 2017). The retail sector, composed of smaller businesses, based on a Chinese victim survey of businesses, tends to fall victim to 'theft by customers'; whereas the wholesaling sector, composed of larger businesses, may fall victims to 'fraud by outsiders' (Broadhurst et al. 2013).
3) Business location. Urbanisation has been associated with crime, with urban residents having fallen victim to crime twice as often as those of non-urban areas (Kalidien et al. 2011). The number of registered crimes per 1000 inhabitants aged 12–79 is almost three times higher in urban municipalities than non-urban areas, in the Netherlands (Eggen and Kalidien 2008). Businesses can also be concentrated in certain geographic locations. Thus, those in the service sector are usually located in the most urbanised part of the Netherlands (Sillen 2014). Accordingly, we analyse the possibility that fraudsters focus on businesses in specific locations (Beasley et al. 2000).
4) Seasonality. In line with the RAT, the relationship between crime and seasonality has been established by previous research (Falk 1952; Cohn and Rotton 2000). Falk (1952) found that crimes that have specific targets (e.g., people) are at a maximum in the summer months; whereas crimes against property (e.g., burglary) are not influenced by seasonality. In general, crime peaks around the holidays, in December, and in the summer months (Cohn and Rotton 2000). The relationship between seasonality and fraudulent attempts against businesses has hardly been investigated previously, but similarly to previous research, the routines of businesses that are linked to seasonality could affect fraud attempts. We propose that businesses might experience low staffing levels during the summer months, staff members might be covering jobs outside their usual expertise, and temporary staff might be employed. These factors should increase the likelihood of success of fraudulent attempts.

Rational Choice Model

While RAT emphasized mostly victim vulnerabilities, the Rational Choice Model (RCM) underscored the rational decision-making process of offenders. This means that an individual acts based on balancing of costs against benefits in a way that promotes personal benefit (Simon 1955).

The Rational Choice Model was adapted from economics to the explanation of crime by Cornish and Clarke (2014). It states that crime is purposive behaviour. The benefits of crime, from the offender's perspective, are commonplace matters, such as money, status, sex, and excitement. Offenders are reasoning actors who weigh means and ends, costs and benefits and take a rough decision for that course of action that seems to yield most benefits. The RCM of crime assumes that offenders are rational decision-makers, but, more than its economic predecessor, it states that this is a 'bounded' or 'limited' rationality (see also Gigerenzer and Goldstein 1996). Criminal's choices are not long-term wise decisions, as they are highly constrained by many factors, such as offenders' abilities, and the availability of relevant information (Cornish and Clarke 2008). Research supports the RCM of crime, for many types of crime, among which ICT-related crime, burglary, robberies and traffic behaviour (Cromwell and Olson 2006; Nicita and Benedettini 2009; Cornish and Clarke 2017).

RCM predicts that there would be a relationship between efforts and rewards. When more efforts are taken, more rewards are expected. For example, in their study of robberies, Van Koppen and Jansen (1998) found that the physical distance between the offence and the home of the offender does not influence the success rate of robbery. But the financial gains are, however, much higher in the robberies committed far away.

Something similar may be hypothesised for fraud: the more international the fraud, the larger the expected benefits. Fraud that involves foreign bank accounts has been gradually increasing since 2009. For instance, in the UK, this type of fraud was estimated to involve £122 in 2009 and £174.8 in 2018 (UK Finance 2019). Having the money transferred to a foreign bank account is interesting from the fraudster's point of view. International crime is, in practice, harder to investigate and to prosecute, and it takes a lot of time (UK Finance 2019; Brenner and Schwerha 2001; Brown 2015). As a result, it is harder to block a foreign bank account, and it's harder to find who is behind that account.

We are hypothesizing that organising a transfer to a foreign bank account means more effort on the part of the offender. 1). In general, it requires better organising skills and more steps to deploy activities on an international level. 2) Opening a foreign bank account often requires additional documents in comparison with a local account and costs more money (Consumer organisation 2020). It usually means dealing with several languages. A recent study indicates that most foreign bank accounts belong to local money mules (EUROPOL 2020). In this case, the money often needs to be transferred back to the Netherlands (or wherever the fraudster is located), which means additional steps are required to benefit from crime carried out. Accordingly, for the present study, we expect that when offenders took more efforts, they also expected higher benefits.

Rational choice and the routine Activity theory are complementary theories of crime science focusing on a rational—though impulsive and opportunistic—offender who searches or takes advantage of opportunities in a way that maximizes benefits but also—importantly—minimizes effort and risks. Rational choice concentrates on the weighing process of an offender, routine activity on the context and the situations with their opportunities and risks, and which bring together potential offenders and victims at specific places and at specific times. It is within these situations that rational decisions are taking place. Of course, the outcomes of these decisions are determined by many others in these situations, the guardians, the potential victims and others who are present in various formal or informal roles. For more extensive discussions we refer to Felson (2017) and Miro Llinares (2014).

Crime scripts

Crime scripts have been proposed as a methodology to analyse relatively various categories of crimes (Cornish 1993; Borrion 2013; Dehghanniri and Borrion 2019). A crime script describes a sequence of steps involved in a specific crime: precursors, transactions, and the aftermath. A crime script should capture all relevant aspects of the modus operandi and the execution of a crime (Clarke and Eck 2005). They can have a variety of forms. For instance, potential scripts describe hypothetical sequences of actions, performed scripts describe a sequence of events that has occurred in the past. Crime script analysis has been used to study a wide range of specific crimes (Cornish 1993). Scripts have been applied relatively often to cybercrime and fraud, perhaps because these are often slightly more complex crimes (for a review see Dehghanniri and Borrion (2019)). In the present study, an important goal of our script is to gauge the amount of effort put into each specific form of fraud.

Research objectives

The present study will address five questions:

1) What are the crime scripts of the three types of fraud, i.e., CEO-fraud, fraudulent contract, and ghost invoice?
2) Are the following business characteristics: business service orientation, business size, business location, and seasonality, related to the three types of fraud, in line with the Routine Activity Theory?
3) Are fraudster characteristics related to the three types of fraud, as predicted by the Rational Choice Model of crime?

4) With what degree of accuracy can one predict the requested amount of money by a fraudster, and subsequently whether the fraudulent attempt is realised?
5) What preventative measures did targeted businesses put in place?

The present research is a quantitative study of 300 fraud cases targeting Dutch businesses using RAT, RCM and the crime script approach. We examine three specific types of fraud: CEO-fraud, fraudulent contract, and ghost invoice. These three types are selected in line with the Fraud Helpdesk (FHD)'s focus on a) two frequently used 'traditional' forms of fraud and b) one 'modern' form.

a) Fraudulent contracts and ghost invoices have been major plagues of Dutch businesses for many years. In the Netherlands, the financial cost of these two types of fraud was estimated to be around €410 million annually (Moolenaar et al. 2011).
b) More recently, CEO-fraud has emerged as a serious new threat with significant financial costs.

In 2017, the FHD registered 20,371 incidents of around 100 different types of fraud. These three selected types of fraud constituted 23.3% of the incidents and were responsible for 10.3% of the monetary losses of Dutch businesses in 2017. More generally, they are also responsible for a high proportion of the total financial loss from fraud in Europe (Bloem 2012; Huisman and Bunt 2009; EUROPOL 2018).

Methods

Sampling strategy: The Fraud Helpdesk data

The Fraud Helpdesk (FHD) (https://www.fraudhelpdesk.org/) was our primary source of information. The FHD is a Dutch non-profit organisation that registers financial crime—attempts or realised, and cyber-enabled or otherwise. It also provides advice to victimised businesses on measures to minimise costs of crime (e.g., financial, reputational). It has the most comprehensive data on financial crime, including around 100 different types of fraud in the Netherlands. The FHD also keeps records that detail the discovery and prevention of fraud.

The data that was coded in the present study is based on information provided by victimised businesses who report the fraud to the FHD. It is similar to the police records. Employees of the FHD note what happened, try to get some information that may help to identify similar types of fraud, and note victim information to be able to re-contact the business if necessary. All this information is confidential. To guarantee anonymity, all information in the present study was coded on the location of the FHD in an anonymous digital dataset.

The FHD does not collect additional information of the businesses, besides the name and some contact information. Accordingly, we collected additional information, on the respective victimised businesses via their websites, on their economic sector and industry (to determine the service orientation), business size and business location.

Since collecting additional information on these businesses was time-consuming, we decided to select 100 cases randomly for each type of fraud in this research project. With the use of the website http://www.random.org, three sets of 100 random numbers were generated. Accordingly, from the 136 cases of CEO fraud), 1294 cases of Acquisition fraud, and 3205 cases of ghost invoices in 2016, one-hundred cases are randomly selected. Due to missing values, the numbers analysed may vary, the numbers on which the percentages are based are indicated clearly in the tables.

Besides FHD data, we also used information from Statistics Netherlands, the official statistics office of the Netherlands to compare the data from the present study with national statistics (Statistics Netherlands 2019).

Concepts and analysis

The definitions and the coding of the concepts are presented in Table 1.

Location and effort

We assumed that fraudsters put more effort into a scam when they used a foreign bank account and that the further away this account was, the more effort they had to put into it. It is important to note that the offender does not necessarily have be in the place where the bank account is located. Perhaps a money mule is there to help him. However, this type of organization that includes a foreign bank account indicates, we believe, that more effort went into planning the fraud. Also. Many of the emails are in English, not in Dutch. Two real-life cases of fraud attempts using a Dutch bank account and three fraud attempts with a foreign bank account are provided to support this assumption. All three cases are in the FHD database, and one is a court case (the Pathé case). We chose CEO-fraud as these cases most often use foreign accounts (as shown later, Additional file 1: Table S6). In each case, the fraudster is referred to as 'Otto#', who often pretends to be the senior manager, who sends a request to his so-called employee or subordinate, probably from a financial department.

Table 1 Definitions and coding of the concepts in the bi-variate and logistic regressions

Dependent variable	
FRAUD, as defined by the FraudeHelpDesk	1) A CEO-fraud occurs when an employee receives an e-mail or a phone call from someone impersonating the Chief Executive Officer (CEO) or the Chief Financial Officer (CFO) to transfer a substantial amount of money to a foreign bank account[a] 2) Fraudulent contracts: advertising agencies approach entrepreneurs offering services (e.g., advertisements in magazines and/or websites) via a phone call or a ghost note; the entrepreneurs are tricked into agreeing to new contracts without being aware of the obligations attached 3) A ghost invoice is a fraudulent invoice 'Type of fraud', in the logistic regression, was coded into two dummies: CEO fraud and Contract fraud (including both fraudulent contracts and ghost invoice) (both: 0 = no, 1 = yes)
Primary method of communication	The contact between the fraudsters and targeted businesses is coded as 1 = email, 2 = offline post, 3 = telephone
Routine activity concepts	
Service orientation	Based on the type of activities as determined from the business' website, we determined the following two variables 1) Economic sector is often operationalised in four sectors. These are: (i) *primary sector*—the retrieval and production of raw materials; (ii) *secondary sector*—the transformation of raw or intermediate materials into goods; (iii) *tertiary sector*—the production of services instead of end products; and (iv) *quaternary or service sector*—the production of knowledge-based services (Kenessey 1987) 2) Industry. Statistics Netherlands codes industrial sector according to a 'SBI 2008—Standard Business classification' (Statistics Netherlands 2018c), which is almost identical to its European equivalent (EUROSTAT 2008). In a logistic regression analysis, the seven largest categories (equal or higher than 5%) were recoded into dummies. There were: (i) business services; (ii) wholesale and retail trade, repairs; (iii) construction; (iv) manufacturing; (v) human health and social work activities; (vi) information and communication technology; (vii) logistics
Business size	Business size was categorised as self-employed (coded as 1), small (coded as 2 = 2–49 employees), medium (coded as 3 = 50–99 employees), large (coded as 4 = 100–250 employees), and very large (coded as 5 = 250 employees and more)
Business location	We coded the province in the Netherlands in which the victim was located. There are 12 provinces in the Netherlands
Season	This was coded based on the date the fraudster first contacted the targeted company In the logistic regression 'season of fraud attempt' was recoded as two dummy variables 'spring' (0 = no, 1 = yes) and 'summer' (0 = no, 1 = yes), which were the two seasons that appeared to be the most relevant
Rational choice concepts	
Effort	1) Crime script. The type of fraud based on its crime script. We used the 'universal script', from Cornish (Cornish 1993: 41, Fig. 4), leaving out the steps: 'entry' and 'exit'. This includes the method of communication Primary method of communication: the contact between the fraudsters and targeted businesses is coded as 1 = email, 2 = offline post, 3 = telephone 2) Location of the bank to which the money is to be transferred. This was coded into four categories: Netherlands (coded as 1), Europe (coded as 2), Hong Kong (coded as 3), and USA (coded as 4). Originally, we coded 'Asia' but this appeared to be only Hong Kong, and 'North America', included only USA. We wanted to code the Netherlands separately, and the rest of Europe involved many different countries. For more details about the countries within Europe, see Table 6, online supplement. We assumed that the further away the bank, the more effort fraudsters put in the fraud attempt. In the logistic regression, Netherlands and Europe were combined and Hong Kong and the USA were combined into single categories
Benefits	This is measured in terms of the amount of money requested and whether it is paid. Information on whether the business paid was also coded (0 = no, 1 = yes). The amount of money requested by the fraudsters was noted in Euro (€) In the regression analysis we used the logarithm (base 10) transformation to reduce skewness, when 'amount of money' is used as the dependent variable

[a] See: https://www.fraudhelpdesk.org/

Dutch bank accounts

(1) Otto1 pretends to be a manager requesting his subordinate to transfer about €6500[3] to a Dutch bank for 'an event'. They exchange three emails of about 1 or 2 brief sentences, all on the same day, from 13:27 until 17:07.

(2) Otto2 similarly pretends to be a manager and asks requests his subordinate to transfer about €100 to a Dutch bank, in poor Dutch and without explanation. They exchange three brief emails, all on the same day, from 15:15 to 16:14.

To summarize, these fraud attempts are simple attempts that did not require a lot of work in terms of email correspondence or storytelling to justify the financial transaction.

[3] We use less specific information in order not to disclose any private information.

Foreign bank accounts

(1) Otto3 requests the director of a Dutch branch of an Italian firm to transfer money for a large transaction, of about €400,000 from his Italian firm to Hong Kong. They exchange 19 emails and Otto emails an invoice. This also happens on the same day, from about 14:30 to 17:00.

(2) Otto4 pretends to be the manager and asks his employee from Finance to transfer about €500,000 to an account in Hong Kong. There are at least 6 emails. These emails are relatively long, and Otto does a good job of explaining why the payment is necessary. The documentation covers at least 5 pages of emails and annexes on the payment details. This email exchange started on a Thursday afternoon and ends about 24 h later.

(3) Otto5 and his friends defraud the Pathé cinema for a total of €19,200,000 (Rechtbank Amsterdam. 2018). This became a well-publicised case. There was an extensive email exchange, several people were involved, at least two from Pathé. There were at least 22 emails, and the entire fraud started on 8th March 2018, and was terminated on 28th March, 2018. The money was transferred to a Dubai account, in several tranches.

Overall, when comparing the fraud attempts using Dutch accounts versus foreign accounts, fraudsters seem to invest more time and effort in writing emails and providing explanations in the context of a foreign bank account. We assume this effort leads to more knowledge of the targeted business and a better justification for the necessity of the money transfer. These observations underpin our hypothesis that when bank accounts are in a foreign country, fraudsters put more time and effort into the attempt.

Crime scripts

The concept of crime script was used to describe the general communication tools used in the fraud incidents of each type of fraud, from the point of view of the offender, as it appears from the records of the Fraud Helpdesk. It should be noted that the Fraud helpdesk, in fact, categorised the different types of fraud that victims report in 100 different categories. Accordingly, they have a quite fine-grained system to categorise fraud. These categories are based on the communication tools used in the fraud. Therefore, the crime presented is a more detailed description of what is already a quite precise categorization of incidents in quite homogenous categories. Therefore, a more complex approach to detect similar scripts, such as (Beauregard et al. 2007) performed was unnecessary in our case. Basically, the Fraud Helpdesk already accomplished this task.

Our data analysis consists of cross-table analysis and two multivariate analyses, including logistic regression and multivariate regression. A binary logistic regression is useful when one models the event probability for a categorical variable with two outcomes, which is our case when predicting whether a victimised company paid or not. Multivariate regression is used when the dependent variable has more than two values, which is our case when analysing the amount of money requested by fraudsters (Hays 1984).

Ethical committee. Permission for the study was granted by the Ethical Committee of the faculty of Behavioral and Management and Social Sciences of the University of Twente under number 17,682.

Results

The crime scripts of the three types of fraud

The crime scripts can be described as follows (Table 2). The first step is the same for each type of fraud and consists of the selection of the victims, in this case, businesses. The fraudsters then need to research the businesses, to gain trust at the time of contact. In the case of CEO-fraud, the research needs to be extensive, as the fraudster is posing as the CEO, who ought to have a great knowledge of the company. In the case of a fraudulent contract and a ghost invoice, extensive research is unnecessary. In these cases, the most important matter is knowing the targeted businesses' types of business and contact information. The next step for ghost invoices is to draw up and send invoices. Sometimes fraudsters would use real invoices and alter the bank account. Sometimes they would fabricate entirely new invoices. Next, they have to wait until these get paid. In our sample, all ghost invoices are sent by regular post (100%, Table 3). In the other two types of fraud, there are more extensive contacts between the fraudsters and the targeted businesses. CEO-frauds are conducted usually via email (94.9%); whereas fraudulent contracts are usually drawn over the telephone (88%) (Table 3).

In fraudulent contracts, in sharp contrast, most attempts are via telephone. Usually, after conducting some research on a targeted company, the fraudster approaches the business by offering an advertising opportunity. There are two ways in which this fraudster could try to get an employee to agree to such an offer: i) recording a verbal agreement (via telephone), or ii) sending a written contract that needs to be signed. In the case of the telephone call, the employee is completely unaware that the phone call is being recorded.

Table 2 Crime scripts by type of frauds

Script scenes[a]	Script actions: CEO-fraud	Script actions: Fraudulent contract	Script actions: Ghost invoice
Preparation	Look for and select a potential company	Look for and select a potential company	Look for and select a potential company.
Instrumental precondition	Conduct extensive research on the company	Conduct minimal research on the company	Conduct minimal research on the company
Instrumental initiation	Spoof the email address of the CEO	Approach the business and persuade the business to accept an advertisement opportunity. Make sure there is a verbal or a signed agreement; this is the contract	Make an invoice for the company? - Use a real invoice and alter the bank account - fabricate an entirely new invoice
Instrumental actualization	Contact the financial employee whilst posing as CEO of the company. Send several emails Request a money transfer to, generally, a foreign bank account	Start sending invoices to the business per payment term	Send the invoice to the company
Post-condition	Push the employee to make the transfer	Push the business to pay the invoices since there is an agreement	Wait and check whether the business pays the invoice

[a] Based on the 'universal script', Cornish (1993: 41, Fig. 4)

Table 3 Main communication tools used in the fraud incidents by type of fraud (in %)

Communication tools	CEO-fraud[a]	Fraudulent contract	Ghost invoice
Email	94.9	3.0	0
Offline post	0	9.0	100.0
Telephone	5.1	88.0	0
N	98	100	100

[a] Chi Square = 500.8; df = 4, p < .0001

In the case of a written contract, they may fall into the trap and sign the contract.

What then follows is a series of invoices that the fraudster sends to the company, which state that the business has a subscription on, for example, an advertisement campaign. When the business tries to contact the fraudster, the reply depends on the type of agreement. In the case of the recorded phone call, the fraudster sends a phone call recording (mostly tampered with), in which an employee agrees to a subscription. In the case of the contract, there are some provisions in small prints, hidden in the contract that state, once signed, the business has agreed to a subscription. Officially, these contracts are legal, and thus the fraudster can send a debt collection agency to collect money from the business (Huisman and 2009).

CEO-frauds, mostly executed via email, can be from any physical location globally. The most common step after having identified the targeted business is spoofing the CEO's email address, by making a slight change in the CEO's name (that is, in the first part of the email address) in the actual email address that is hard to identify. Examples are replacing a '0' with an 'o' or a capital 'I' with a lowercase 'i'.

In the next step, the fraudster sends an email to an employee in the finance department posing as the CEO and asking the employee to transfer a specific amount of money to a bank account. When the employee asks questions, the fraudster pushes the employee to make the transfer quickly, by stating that this transaction has priority and the paperwork can be arranged afterwards. The employee is sometimes given the choice to call a law firm to verify the transaction, which is, of course, involved in the fraudulent attempt. Sometimes, there can be telephone contact (5.1%; Table 3). This is, however, rare, as telephone numbers can be checked. Fraudsters thus need to speak a specific language, and questions can easily be asked, resulting in a low success rate. Therefore, fraudsters often insist that they cannot be reached by telephone ('I am in a meeting', the telephone was lost or stolen) and that communication needs to be done by e-mail.

Routine Activity Theory: opportunities and business routines and type of fraud

Service orientation

Two indicators measured service orientation: economic sector and industry category. In terms of the economic sector, fraud occurs the most frequently in the tertiary sector. It has sustained 62% of all reported CEO-frauds and 73% of ghost invoices. However, this section has 73.7% of the employees of all businesses in the Netherlands. This implies that fraudsters do not target businesses in the tertiary sector disproportionally (Additional file 1: Table S1).

The differences in fraud concentration follow, to a large extent, the distribution of businesses over different

Table 4 Business size by type of fraud and business size in the Netherlands in 2016 (in %)

Business size	CEO-fraud	Fraudulent contract	Ghost invoice	Businesses Netherlands[a]	Number of employees (except self-employed)[b]
Self-employed (1)	0	44.0	26.3	79.1	–
Small (2–49)	30.0	51.0	61.6	19.8	31
Medium (50–99)	15.0	2.0	8.1	.41	8
Large (100–250)	25.0	2.0	3.0	.46	11
Very large (250 and more)	30.0	1.0	1.0	–	50
N, %	100	100	99	100%	100%

Chi Square = 148.7; df = 8, p < .001 (computed with the three types of fraud)

[a] Statistics Netherlands (2018a)

[b] Statistics Netherlands (2016)

types of industry in the Netherlands. In two cases, there appears to be a disproportionate concentration. First, CEO-fraud is targeting businesses in the manufacturing industry more frequently—18% of all CEO-frauds occur is this branch, while this industry constitutes only 4% of all businesses in the Netherlands. Second, fraudulent contracts often occur in the human health and social work industry—18% of all fraudulent contracts target this industry, while this industry constitutes only 8.8% of all businesses in the Netherlands (Additional file 1: Table S2).

Business size

In terms of business size, the larger a company, the more likely it is to suffer from an attempted CEO-fraud (Table 4). Over half of the businesses (55%) that reported CEO-fraud are large (100–250 employees) and very large (250 employees and more), but they constitute only .5% of all businesses in the Netherlands. Constituting only 19.8% of all businesses, small businesses (2–49 employees) are more likely to be the victims of fraudulent contracts (51%) and ghost invoices (61.6%) than CEO fraud.

Geographic location of businesses

Frauds are reported most often in three provinces: North-Brabant, South-Holland, and North-Holland. Together, these produce 64% of the total national business turnover. We see a slight concentration of CEO-fraud in these three provinces. Fraudulent contract and ghost invoices are less concentrated but spread more uniformly over all provinces, in the same proportions as the business turnover (Additional file 1: Table S3).

Seasonality

There are clear differences between the three types of fraud in terms of the season of their occurrence. 73% of all CEO-frauds occur in the summer, 72% of the ghost invoices are concentrated in spring, and fraudulent contracts are spread more uniformly over the year (Table 5).

The Rational Choice Model of crime: associations between effort and benefits

The Rational Choice Model of crime predicts that when offenders take more effort, they expect higher rewards. Accordingly, our two measures of effort, namely type of fraud and location, implying distance from the Netherlands should be related to requested amounts of money.

Type of fraud and benefits

The description of the crime scripts above shows that a CEO-fraud requires extensive effort, while a ghost invoice is 'a one-time shot in the dark'. A fraudulent contract, in terms of effort, situates in between. As expected, in CEO-fraud, fraudsters requested much higher demands of money, in fraudulent contracts, the requested amount was lower, and in ghost invoices, it was quite low. In CEO-frauds, the median amount of money was €91,147, for fraudulent contracts, this was €361 (49% between €200–€ 499), and for ghost invoices, this was €175 (65% less than €199) (Additional file 1: Table S4). Interestingly, in CEO-frauds, all amounts were higher than €10,000;

Table 5 Seasonality by types of fraud (in %)

The season when fraud was committed	CEO-fraud	Fraudulent contracts	Ghost invoices
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 (computed with the three types of fraud)

Table 6 Prediction of the amount of money requested by fraudsters (unstandardized Coefficients from a multiple regression analysis; N = 226)

Variables in the analysis	B		Std. Error
Constant	**2.60**	**	**.18**
1. Business services	− .01		.07
2. Wholesale and retail trade, repairs	− .06		.07
3. Construction	− .11		.12
4. Manufacturing industry	− .16		.11
5. Human health and social work activities	.04		.10
6. Information and communication, ICT	.01		.12
7. Transport and storage	.01		.13
8. Business size	.0008	*	*.00*
9. Sector the defrauded SME is active in.	− .12		.07
10. CEO fraud	2.01	**	*.09*
11. Contract fraud	.21	**	*.07*
12. Fraud in springtime	− .21	**	*.07*
13. Fraud in summertime	.00		.08
14. Fraudster in USA or Hong Kong	.13	**	.03

Missing values: 29 missing from lack of information on where the fraudster is operating from and 72 cases had no information on 'amount asked' by the fraudster

Statistically significant variables are printed in italized

* p < .05; ** p < .001

and in 11 cases, fraudsters asked for more than €100,000. The highest was €425,000.

Did the attack succeed or fail?

On average, 9% of the fraud attempts were successful—CEO-frauds (11%, N = 99), fraudulent contracts (8% N = 100), and ghost invoices (7% N = 100; Pearson Chi Square = 1,1; df = 2 p = .58). The relationship between the type of fraud and the requested amount of money was not affected by whether businesses paid or not. Furthermore, we found no relationship between the amount of money requested and whether the business paid (p < .05 within each type of fraud) (Additional file 1: Table S5).

Location and requested amount of money

Most fraudsters operated from the Netherlands, namely 57.3%, 20.3% operated from elsewhere in Europe, 8.3% in Hong Kong, and 4.3% from the USA (N = 271).

The type of fraud that takes the most effort, namely CEO fraud, almost always requested the money being transferred to a foreign bank account: in only 1.4% of the CEO-frauds, the request was to send money to a local bank account, while this was 100% for fraudulent contracts and 71% for ghost invoices (Additional file 1: Table S6).

As expected, the location of the bank account was strongly correlated to the amount of money requested. When fraudsters have a Dutch bank account, only 2.3% of the fraud attempts fraudsters request €10,000 or more. But when their bank account is elsewhere in Europe, this is 73%; and when it is in Asia (always Hong Kong) 100%. When they seem to work from the America (always the USA), based on their bank account, the requested amounts are between €500 and €9999 (Pearson Chi Square = 239.2, df = 9, p < .0001; Additional file 1: Table S1). These findings are indicative of a linear relationship: the lowest amounts are requested in the Netherlands, and the requested amount increases when the account is farther away from the Netherlands.

With what degree of accuracy can one predict the requested amount of money by a fraudster, and whether the fraudulent attempt is realised?

A multiple regression analysis has been conducted to investigate whether the amount of money requested relates to independent variables (Table 6). Because of the relatively high number of variables for a sample of 300 cases, not every variable could be used. However, we used all variables that might be related to the dependent variable given the findings of the bi-variate analysis. The R square adjusted was .91 (F = 154.5, p < .001). Five variables were strongly correlated to the amount of money requested, largely corroborating the bivariate analysis. First, type of fraud was the main predictor: fraudsters ask for more when they engage in CEO fraud, and much less when they engage in contract fraud, in comparison with ghost invoices. Secondly, they ask for more when the potential victim is a large business, in comparison with smaller businesses. Third, they ask for less money when the fraud is conducted in springtime, probably reflecting the fact that during this time, fraudsters engage relatively often in sending ghost invoices, for which they only request relatively small amounts of money. Finally, location, as an indicator of effort, matters. When fraudsters' bank account is in the USA or Hong Kong, fraudsters request larger amounts of money. Neither the economic sector or industry category are related to the amount of money requested, controlling the other factors in the analysis.

A logistic regression analysis was conducted to investigate whether variables used correlated to the actualisation of fraudulent attempts (payments from businesses) (Additional file 1: Table S1). Again, because of the relatively high number of variables for a sample of 300 cases, we did not use every variable in the analysis but used all variables that could be related to the dependent variable given the bi-variate findings. 15 variables were entered in the logistic regression. These included the 14 independent variables used in the multiple regression (Additional file 1: Table S2), and the amount of money asked. None of the variables had any impact on whether the business paid.

There was one exception on the verge of statistical significance: during summertime, the likelihood of being paid is only one-fifth of what it is the rest of the year (p = .09).

What preventative measures did targeted businesses put in place?

In 91% of attempted frauds, the attempt was usually discovered when attentive employees noticed something was either 'weird' or 'wrong'. With CEO-fraud, in 27 cases, these employees noticed that the requested amount was absurd. More specific reasons were: the employee noticed that contacts with the offender or the email were 'weird' (4 times); the employee noticed that similar previous emails had been send (4); the offender did not know the company rules (3); the employee called the CEO for confirmation (2); the employee saw a faulty email address (2); the employee had previous knowledge on CEO-fraud (1), and the employee noticed that the company that was mentioned by the offender did not exist (1). One CEO-fraud was carried out by an ex-insider, and the employee noticed that this person did not work at the company anymore (1). Other means of fraud detection include the ICT department saw similar fraudulent emails before (2); the bank noticed something was wrong (1), and another company noticed (1) (Additional file 1: Table S3).

With the 9% of businesses that paid, employees noticed that they were often defrauded after a second contact with the fraudsters. In three cases, they were alerted when requests for second payments arrived. In three other cases, financial departments noticed that something was wrong with the payment.

Discussion

This study analyses 300 cases of fraudulent activity, of these 100 cases are from each of the following three categories: CEO-fraud, fraudulent contract, and ghost invoice. Below we discuss the main findings.

1) What are the crime scripts of the three types of fraud?

   Fraudulent contracts and ghost invoices were chosen as they are the old major plagues of Dutch business (Huisman and 2009) and are still conducted via traditional means—all ghost invoices are sent by regular offline post, and 88% of fraudulent contrasts are attempted via the telephone. In contrast, the new threats—CEO-frauds—are largely conducted via a relatively new tool—email (94.9%). Our study aimed to answer five questions. The three types of fraud differ in their script and modus operandi. Ghost invoices are sent by post, and the fraudster just waits until it is paid. In fraudulent contracts, most attempts are via telephone. The fraudster approaches the business by offering an advertising opportunity. The fraudster needs the victim to agree with this offer either by i) recording a verbal agreement (via telephone), or ii) sending a written contract that needs to be signed. Officially, these contracts are legal, and thus the fraudster can send a debt collection agency to collect money from the business (Huisman and 2009). CEO fraud demands more time and effort of the fraudster. The fraudster needs to know enough from the targeted business to simulate for some time being the CEO or CFO. There is sometimes intensive email contact while avoiding telephone contact. In sum, crime scripts differ greatly. The crime scripts show that ghost invoices are relatively easy, fraudulent contracts require more effort and CEO fraud is a more intensive fraudulent method.

2) Are business characteristics related to the three types of fraud, as predicted by the Routine Activity Theory? Five variables measures were indicators of opportunity and routine activities of businesses: service orientation, measured by economic sector and industry, business size, business location, and seasonality.

In the present study, there was no relationship between service orientation or geographic location of the businesses and type of fraud, especially when we compared our figures with the distribution of the targeted businesses with national statistics. Previous research, however, did report a concentration of fraud by service orientation. However, these studies generally did not compare their distribution of fraud cases with the distribution of businesses by industry nation-wide (e.g., Huisman and (2009). No previous research was found with respect to geographic location and fraud.

Business size and seasonality, however, were strongly related to fraud type. Fraudsters clearly take business characteristics and routines into account when executing their acts and thus provide a solid support for RAT.

Fraudulent contracts and ghost invoices focus on smaller businesses (2–49 employees). CEO fraud, in contrast, focusses on larger businesses (100 employees and more). As reported by the Verizon Risk Team (Verizon Risk Team. 2017), different types of fraud target different types of businesses. As mentioned by Huisman and (2009) fraudulent contracts and ghost invoices targeted smaller businesses. Hrncir and Metts (2012) and the global report on fraud (ACFE 2018) also reported that small businesses fell victim to fraud disproportionately. This is also in line with (Coopers 2014) that cybercrime focusses on relatively large businesses.

How does a Routine Activity approach explain these findings? We propose that fraudsters try to find a rough match between their choice of weapon and the selection of a potential victim. Several aspects may play a role. Smaller businesses may have less strict procedures and less advanced administrations, which makes them more vulnerable to ghost invoices and fraudulent contracts (Smith 2013; Laufer 2011). Also, smaller amounts of money probably raise less suspicion, which in turn does not incite employees to carry out checks and controls. The financial means of these businesses are also smaller, accordingly, fraudsters must adapt the requested amounts of money to the potential victims. Furthermore, a small business may not be very alert to the dangers (Hess and Cottrell 2016). According to a security company, '51% of SMB Leaders Think Their Business Isn't a Target for Cybercriminals' (Gross 2018). Finally, of course, there are many more small businesses than large businesses. In the Netherlands, 1% of the businesses are larger than 50 employees (when including the self-employed).

Our findings, in terms of seasonality, support earlier research and show that different types of fraud occur in different seasons (Cohn and Rotton 2000). Again, from a Routine Activity Theory approach, the fraudster's behaviour makes sense: the results show that fraudsters adapt to seasonal business routines. 73% of all CEO-fraud occurs during the summer, as fraudsters could impersonate CEOs who, fraudsters believe, might be on holiday. 10 million of out the 17 million Dutch people are on holiday during this period of time (Statistics Netherlands 2017). 72% of ghost invoices occur in the spring when individuals and businesses are very busy closing the fiscal year. Fraudsters, sending ghost invoices, probably believe that during this busy season, employees tend to pay any unpaid bills in a hurry. As a result, they are less precautious about paying unknown bills. For fraudulent contracts, no pattern was found, and there are no seasons to sign contracts.

3) Are fraudster characteristics related to the three types of fraud, as predicted by the Rational Choice Model of crime?

   Third, supporting the RCM, our findings demonstrate a strong relationship between effort and benefit—the higher the amount of effort involved in committing the crime, the higher the requested amount of money (Cornish and Clarke 2017). Effort was operationalised as the location of bank account—implying distance from the Netherlands—and type of fraud, as the three types of fraud, involved a different level of effort. Each of the three types of fraudulent attempts has similar degrees of 'success' (on average about 9%). But the amounts asked for and received differ significantly. CEO-fraud—the most elaborated form—leads to the greatest financial benefits (always more than €10,000). In the simplest form of fraud, ghost invoices, fraudsters request the lowest amounts of money. Furthermore, we found that the further away the location of the bank account was from the Netherlands, the higher the amount of money that was requested.

   Although we proposed that distance is an indicator of effort and that effort leads to higher requested amounts of money, there may be alternative explanations for the relationship between distance and these requests. First, a bank account abroad does perhaps not always point to the degree of effort an offender invested in the fraud. The type of fraud in itself may lead offenders to select a specific amount of money. For instance, the way most CEO-frauds are framed, for instance, is that an executive buying another company implies a considerable amount of money. Second, if fraudsters for some reason decide to target victims abroad, they are limited in the types of fraud they could commit. For instance, sending ghost invoices from abroad may raise more suspicion than an invoice from a Dutch company. It needs to be noted that the type of fraud is strongly associated with several other fraud and victim characteristics (e.g., means of communication, victim size) making it difficult to distinguish between these characteristics and their impact on, for instance, the requested amount of money. Studies with larger samples and more diverse types of fraud may enable us to distinguish between the impact of the different factors.

4) With what degree of accuracy can one predict the requested amount of money by a fraudster, and whether the fraudulent attempt is realised?
   Several factors predicted the amount of money requested by fraudsters. The amount of money requested is higher for large businesses, in CEO fraud, and slightly higher for contract fraud in comparison with ghost invoices. During springtime (mostly ghost invoices) fraudsters request lower amounts of money. In sum, when they perceive businesses can pay (in line with opportunities and RAT), or when they put more effort into a fraud attempt (rational choice), fraudsters ask for more money. Previous research found similar relationships between effort and expected rewards. In their study of robberies, Van Koppen and Jansen (1998) found that in terms of robbery, distance does not affect the success rate, yet the financial benefits of robberies committed far away are much higher. Rengert and Wasilchick (1985)'s research on burglars found a similar relationship between effort and benefit.

On average, for all types of fraud, about 9% of the targeted businesses paid. It was difficult to predict whether a business would pay. A multivariate analysis has established that only one risk factor, namely seasonality, was (marginally) correlated to the likelihood of paying—in the summer, the likelihood of being paid is a fifth of the average of the other seasons. This might be related to the fact that in the summer, 10 out of the 17 million Dutch are on holiday, leading to a slowing down of all activities, including paying bills (Statistics Netherlands 2017). Apparently, no type of business or business characteristic protects businesses from paying in case of a fraud attempt.

5) What preventative measures did targeted businesses put in place?

We found some indications on what helped businesses avoid paying. In all cases, when nothing was paid, both online and offline, the fraud was prevented by vigilant employees who noticed something unusual. More generally, for each type of fraud, be it cyber-enabled or not, in the end, an individual employee must be involved to make a payment. Thus, fraudulent activities, in general, could be prevented by vigilant employees. Therefore, to mitigate these activities, businesses need to offer more effective training and support to enable better job performance of their employees. The fraud Helpdesk provided some simple but effective measures. These are i) always pay attention with verbal promises; ii) check carefully before signing anything; iii) always check the text (including and the lower-case text); and iv) do not sign and return 'just' a fax, e-mail or postal item (Fraudehelpdesk.nl 2018). Furthermore, to prevent CEO-fraud, guidelines about how to deal with unusual requests are needed, e.g., an extra step in payment procedures to verify requests. Employees should not feel alone but should always be able to share and discuss payment requests with an executive. Finally, even when a sum of money has been transferred, if one acts quickly, banks could sometimes hold the transaction prior to its finalisation.

It should be noted that, until recently, contract fraud was 'almost' legal, in the sense that it was very difficult to prove fraudulent intent on the part of the fraudster. Fraudsters sometimes use collection agencies to pressurize companies to pay, which further complicates things for victimised companies (Huisman and 2009). Since July 2016, there is a new law in the Netherlands that aims to protect businesses against 'misleading commercial practices between organizations' (Hijma 2017). This new law stipulates that it is up to fraudsters to prove that they have fully and correctly informed the entrepreneur. If this is not the case, it will be easier to declare a contract being invalid. In case of violation of the law, a maximum prison sentence of two years can be applied. Unfortunately, according to the data of the fraud Helpdesk, this new legislation has not changed anything; and thus, contract fraud and ghost invoices are still sent to companies as frequently as before (van Eck 2018).

Limitations

Our research has its limitations. There is no way of knowing to what extent our sample is representative of businesses that are targeted by fraudsters. We assume that we investigated a representative sample of the relatively serious attacks, assuming seriousness is an important selection mechanism for reporting a crime as many victim surveys indicated (Skogan 1984). But we cannot be certain about this.

Some variables, such as the location of a fraudster and the company's service orientation could, in future research, be operationalised with more prevision. To be able to discuss the extent to which businesses that are targeted by fraudsters differ from Dutch averages, we tried to find figures from Statistics Netherlands on factors that are measured in this research. We were able to find figures concerning the numbers of employees, businesses, and 'business turnover' but not for all businesses. This is because figures on business turnover are published by province, not by business industry or size; and the number of businesses was by business size, not by the economic sector.

Conclusion

In sum, to mitigate fraudulent activities and support employees, businesses need to offer more effective training and support to enable better job performance of their employees. The FHD has already provided some simple but effective measures. These are i) paying attention with verbal promises; ii) checking carefully before signing anything; iii) checking the text (including and the lower-case text); and iv) not signing and returning a fax, e-mail or postal item (Fraudehelpdesk.nl 2018). To prevent CEO-fraud, guidelines about how to deal with unusual requests are now needed, e.g., an extra layer of management to verify requests. Employees should not feel isolated but should always be able to share and discuss payment requests with an executive. Additionally, even when a sum of money has been transferred, if one acts quickly, banks can sometimes hold the transaction before it is finalised. For small businesses, which tend to suffer from fraudulent contracts and ghost invoices, Hrncir and Metts (2012) provide four preventive measures. These are i) owners and managers should set the tone that honesty and integrity are required by displaying these traits in daily activities; ii) establishing formal hiring practices; iii) having appropriate internal control procedures, e.g., have different individuals in charge of different stages of payment; and iv) restricting access to business issued credit cards only to key employees.

Supplementary information

Supplementary information accompanies this paper at https://doi.org/10.1186/s40163-020-00119-4.

Additional file 1. Additional tables.

Abbreviations

FHD: Fraud Helpdesk; RAT: Routine Activity Theory; RCM: Rational Choice Model.

Acknowledgements

The authors would like to thank Fleur van Eck, director of the he Fraud Help Desk (FHD), and Elmer Lastdrager, Cynthia Hukon and Jos Kerssen of the FHD for their willingness to provide the opportunity to use data from the Fraud Helpdesk and their advice during the data collection.

Authors' contributions

MJ wrote the article end performed the analyses. VW critically edited the text. MS developed a coding scheme, together with MJ and collected the data. All authors read and approved the final manuscript.

Authors' information

Marianne Junger is full professor of Cyber Security and Business Continuity at the University of Twente, m.junger@utwente.nl. Her research focusses the human factors of fraud and of cybercrime, more specifically in victimization, phishing, disclosure and privacy issues. The aim is to develop interventions that will help to protect users.

Victoria Wang is a Senior Lecture on Security and Cybercrime in the Institute of Criminal Justice Studies (ICJS), University of Portsmouth, UK, victoria.wang@port.ac.uk. Her current research ranges over cyber/information security, surveillance studies, social theory, technological developments and online research methods.

Marleen Schlömer has a MSc in Business Administration. She specialised in finance, and works as a financial expert at A.S. Watson Benelux, marleen-schlomer@gmail.com.

Funding

No funding.

Availability of data and materials

The data will be made available through DANS (https://dans.knaw.nl/en).

Competing interests

The authors have no competing interests.

Author details

[1] Department of Industrial Engineering and Business Information Systems, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands. [2] Institute of Criminal Justice Studies (ICJS), University of Portsmouth, University House, Winston Churchill Avenue, Portsmouth, Hampshire PO1 2UP, United Kingdom. [3] Watson Benelux, 3927 DA Renswoude, The Netherlands.

Received: 13 December 2019 Accepted: 6 June 2020
Published online: 09 July 2020

References

ACFE. (2018). *Report to the nations.global study on occupational fraud and abuse* (p. 80). Austin, TX: Association of Certified Fraud Examiners.

BCC. (2008). *The invisible crime: A business crime survey* (p. 28). London, UK: British Chambre of Commerce.

Beasley, M. S., Carcello, J. V., Hermanson, D. R., et al. (2000). Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms. *Accounting Horizons, 14,* 441–454.

Beauregard, E., Rossmo, K., & Proulx, J. (2007). A descriptive model of the hunting process of serial sex offenders: A rational choice approach. *Journal of Family Violence, 22*(6), 449–463.

Benson, M. L., Madensen, T. D., & Eck, J. E. (2009). *White-collar crime from an opportunity perspective*. New York: Springer.

Bloem, B. (2012). Horizontale fraude in kaart. *Het tijdschrift voor de politie, 75,* 30–34.

Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science, 2,* 6.

Brenner, S. W., & Schwerha, J. J. (2001). Transnational evidence gathering and local prosecution of international cybercrime. *J Marshall J Computer & Info L., 20,* 347.

Broadhurst, R., Bouhours, B., & Bouhours, T. (2013). Business and The Risk of Crime in China. *British Journal of Criminology, 53,* 276–296.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9,* 55.

Brunet, J. R. (2002). Discouragement of crime through civil remedies: An application of a reformulated routine activities theory. *Western Criminology Review, 4,* 68.

Button M, Lewis C and Tapley J. (2009) Fraud typologies and the victims of fraud. Literature review. London, UK: University of Portsmouth. Centre for Counter Fraud Studies, Institute of Criminal Justice Studies. National Fraud Authority.

Clarke RV and Eck JE. (2005) Crime Analysis for Problem Solvers in 60 Small Steps. Washington D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, 150.

Cohen, L. E., & Felson, M. (1979). Social-change and crime rate trends - routine activity approach. *American Sociological Review, 44,* 588–608.

Cohn, E. G., & Rotton, J. (2000). Weather, seasonal trends and property crimes in Minneapolis, 1987–1988. A moderator-variable time-series analysis of routine activities. *Journal of Environmental Psychology, 20,* 257–272.

Consumer organisation. (2020) *Transfering money abroad.* https://www.consumentenbond.nl/betaalrekening/geld-overmaken-naar-buitenland.

Coopers, P. W. (2014). *2014 Information security breaches survey. Technical report.* London: Price Waterhouse Coopers.

Coopers PW (2018) Pulling fraud out of the shadows. Global Economic Crime and Fraud Survey 2018. USA.

Cornish DB. (1993) Crimes as scripts. In: Zahm D and Cromwell P (eds) *Proceedings of the international seminar on environmental criminology and crime analysis.* Coral Gables, Florida: Florida Criminal Justice Executive Institute Tallahassee, FL., 30-45.

Cornish, D. B., & Clarke, R. V. (2008). Rational choice perspective. In R. Wortley & L. Mazerolle (Eds.), *Environmental criminology and crime analysis*. Willan: Abingdon, UK.

Cornish DB and Clarke RV. (2014) *The reasoning criminal: Rational choice perspectives on offending*: Transaction Publishers.

Cornish, D. B., & Clarke, R. V. (2017). The reasoning criminal: Rational choice perspectives on offending. *Environmental criminology and crime analysis* (pp. 29–61). Taylor & Francis Group: Abingdon.

Cressey, D. R. (1964). *Delinquency, crime and differential association*. The Hague, Nl.: Martinus Nijhoff.

Cressey, D. R. (1965). The respectable criminal. *Criminology, 3,* 13–16.

Cromwell, P., & Olson, J. N. (2006). *The Reasoning Burglar: Motives and Decision-Making Strategies*. New York: Roxbury Publishing.

Deevy M and Beals ME. (2013) The scope of the problem an overview of fraud prevalence measurement. Stanford, CA: Fraud Research Center. Retrieved from: http://fraudresearchcenter.org/wp-content/uploads/2013/11/Scope-of-the-Problem-FINAL.pdf, 46.

Deevy M, Lucich S and Beals ME. (2012) Scams, schemes & swindles. A review of consumer financial fraud research. Stanford, CA: Fraud Research Center, 47.

Dehghanniri H, Borrion H. (2019) Crime scripting: a systematic review. *European Journal of Criminology*.

Dorminey, J., Fleming, A. S., Kranacher, M.-J., et al. (2012). The evolution of fraud theory. *Issues in Accounting Education, 27,* 555–579.

Eggen ATJ and Kalidien SN. (2008) Criminaliteit en rechtshandhaving 2007. Ontwikkelingen en Samenhangen. Den Haag, Nl.: Boom, WODC, Ministerie van Jusitie, CBS.

EUROPOL. (2018). *Click here and see how your money disappears—criminal #cyberscams of the 21st century*. The Hague: EUROPOL.

EUROPOL. (2020) *Money Muling*. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/money-muling.

EUROSTAT. (2008) *Statistical Classification of Economic Activities in the European Community, Rev. 2 (2008)*. http://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF.

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

Farrell, G. (2013). Five tests for a theory of the crime drop. *Crime Science, 2,* 1–8.

Felson, M. (1995). Those who discourage crime. In R. V. Clarke (Ed.), *Crime prevention studies* (pp. 53–66). Monsey, NY: Criminal Justice Press.

Felson M. (2017) Linking criminal choices, routine activities, informal control, and criminal outcomes. *The reasoning criminal.* Routledge, 119–128.

Financial Intelligence Group. (2017) From suspicion to action. Converting financial intelligence into greater operational impact. In: EUROPOL (ed). Luxembourg, Lux.: European Union, Publications Office.

Finnerty, K., Motha, H., Shah, J., et al.: (2018) Cyber Security Breaches Survey 2018: Statistical Release.

Fraudehelpdesk.nl. (2018) *Hoe voorkom ik acquisitiefraude? (How to prevent contract fraud?)*. https://www.fraudehelpdesk.nl/fraude-abc/voorkomen-acquisitiefraude/?zoekopdracht=acquisitiefraude.

Gigerenzer, G., & Goldstein, D. G. (1996). Reasoning the fast and frugal way: Models of bounded rationality. *Psychological Review, 103,* 650–669.

Gross A. (2018) 51% of SMB Leaders Think Their Business Isn't a Target for Cybercriminals.

Hays W. (1984) Statistics for Behavioral Sciences. *Psyccritiques* 29.

Hess, M. F., & Cottrell, J. H., Jr. (2016). Fraud risk management: A small business perspective. *Business Horizons, 59,* 13–18.

Hijma J. (2017) Annotatie HR 27 mei 2016, NJ 2017/312 (Van de Booren/Grenkefinance). *Nederlandse Jurisprudentie* 2017.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46,* 189–220.

Hrncir, T., & Metts, S. (2012). Why small businesses fall victim to fraud: Size and trust issues. *Business Studies Journal, 4,* 61–71.

Huisman K and Bunt HGvd. (2009) Misleidende handelspraktijken. Een onderzoek naar de aard, achtergronden en aanpak van acquisitiefraude in Nederland (Misleading commercial practices. An investigation into the nature, background and approach to fraudulent contract in the Netherlands). Rotterdam, Nl.: WODC, Erasmus Universiteit Rotterdam - Faculteit der Rechtsgeleerdheid.

Kalidien SN, de Heer-de Lange NE and van Rosmalen MM. (2011) Criminaliteit en rechtshandhaving 2010. Ontwikkelingen en samenhangen. *Onderzoek en Beleid.* Meppel: Boom Juridische uitgevers:, 574.

Kenessey, Z. (1987). The primary, secondary, tertiary and quaternary sectors of the economy. *Review of Income and Wealth, 33,* 359–385.

Laufer, D. (2011). Small business entrepreneurs: A focus on fraud risk and prevention. *American Journal of Economics and Business Administration, 3,* 401–404.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology and Criminal Justice, 8,* 389–419.

Levi, M., & Burrows, J. (2008). Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey. *British Journal of Criminology, 48,* 293–318.

Miro, L. F. (2014). *Routine Activity Theory, The encyclopedia of theoretical criminology* (pp. 1–7). New York: Wiley.

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,* 159–178.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. London, UK: Home Office.

Montoya L, Junger M and Hartel P. (2013) How 'Digital' is Traditional Crime? *European Intelligence and Security Informatics Conference (EISIC) 2013*. Accessed August 12-14, 2013.

Moolenaar DEG, Nauta B and Tulder FPv. (2011) Kosten van criminaliteit (The costs of crime) Chapter 10. In: Rosmalen MMv, Kalidien SN and Heer-de Lange NEd (eds) *Criminaliteit en rechtshandhaving 2011. Ontwikkelingen en samenhangen (Crime and law enforcement 2011. Developments and connections).* The Hague, Nl.: WODC, CBS, Raad voor de Rechtspraak, Nl.

Murphy PR, Free C and Branston C. (2011) Organizational Culture as a Predictor of Fraud. Waterloo, Canada: Queen's School of Business. http://accounting.uwaterloo.ca/SAF/Documents/Murphy%20paper.pdf.

National Academies of Sciences E, and Medicine (NAP). (2018). *Modernizing Crime Statistics: Report 2-New Systems for Measuring Crime*. Washington, DC, USA: The National Academies Press.

NCJRS. (2017). *Financial Crime Fact Sheet - Office for Victims of Crime* (p. 2). Washingron DC: National Criminal Justice Reference Service (NCJRS).

Nicita A and Benedettini S. (2009) Rational Drivers, Irrational Enforcers, and Road Safety. *SSRN eLibrary*.

Piquero, N. L., & Benson, M. L. (2004). White-Collar Crime and Criminal Careers: Specifying a Trajectory of Punctuated Situational Offending. *Journal of Contemporary Criminal Justice, 20,* 148–165.

Rechtbank Amsterdam. (2018) *ECLI:NL:RBAMS:2018:7881 - Rechtbank Amsterdam, 31-10-2018/7018728 EA VERZ 18-544 (in Dutch)*. Available at: https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:RBAMS:2018:7881.

Rengert G and Wasilchick J. (1985) *Suburgan Burglary: a Time and a Place for Everything.,* Springfield IL USA: Charles C. Thomas.

Schuchter A and Levi M. (2013) The Fraud Triangle Revisited. *Security Journal*: 1-15.

Sillen, K. (2014). Clustering van bedrijven in beeld (clustering of companies). *Economisch Statistische Berichten. Dossier Ecosystemen voor ondernemen, 99,* 14–19.

Simon, H. A. (1955). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics, 69,* 99–118.

Simpson, S. S. (2010). Making sense of white-collar crime: Theory and research. *Ohio St. J. Crim. L., 8,* 481.

Simpson, S., Rorie, M., Alper, M. E., et al. (2014). Corporate crime deterrence: A systematic review. *Campbell systematic reviews, 10,* 250.

Skogan, W. G. (1984). *Issues in the measurement of victimization*. Washington DC: U.S. Department of Justice, Bureau of Justice Statistics.

Smith GS. (2013) Small business fraud and the trusted employee. Protecting against unique vulnerabilities.

Statistics Netherlands. (2016) *Banen van werknemers; bedrijfsgrootte en economisch activiteit (SBI2008), 2008-2014*. Available at: http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=81497NED&LA=NL.

Statistics Netherlands. (2017) Hoogseizoen telt bijna 10 miljoen vakantiegangers (High season has nearly 10 million vacationers). In: (CBS) CBvdS (ed).

Statistics Netherlands. (2018a) *Bedrijven, naar bedrijfstak*. http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=81589NED.

Statistics Netherlands. (2018b) *Geregistreerde criminaliteit; regio (indeling 2013) 2005-2012*. http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=80344NED&D1=0&D2=a&D3=0&D4=a&HDR=G2,T,G3&STB=G1&VW=T.

Statistics Netherlands. (2018c) *SBI 2008 - Standaard Bedrijfsindeling 2008, Version 2018*. https://www.cbs.nl/nl-nl/onze-diensten/methoden/classificaties/activiteiten/sbi-2008-standaard-bedrijfsindeling-2008.

Statistics Netherlands. (2019) https://www.cbs.nl/en-gb.

Sutherland, E. H., & Cressey, D. R. (1974). *Criminology*. Philadelphia, USA: J.B. Lippincott Company.

Tilley, N., & Sidebottom, A. (2015). Routine activities and opportunity theory. In M. D. Krohn & J. Lane (Eds.), *The handbook of juvenile delinquency and juvenile justice* (pp. 331–348). Oxford, UK: Wiley.

UK Finance. (2019). *Fraud the facts 2019. The definitive overview of payment industry fraud* (p. 4). Lononn, UK: UK Finance.

van Eck F. (2018) Acquisitiefraude en wetgeving (Contract fraud and legislation). In: Junger M (ed). Apeldoorn, Nl.

Van Koppen, P. J., & Jansen, R. W. J. (1998). The road to the robbery: Travel patterns in commercial robberies. *British Journal of Criminology, 38,* 230–246.

Van Vlasselaer, V., Bravo, C., Caelen, O., et al. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems, 75,* 38–48.

Verizon Risk Team. (2017) 2017 Data Breach Investigations Report. 10th edition. Verizon. http://www.verizonenterprise.com/DBIR/.

Wolfe DT and Hermanson DR. (2004) The fraud diamond: Considering the four elements of fraud. *The CPA Journal* December.

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

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.