GOWER
Applied Research

INVESTIGATION AND PREVENTION OF FINANCIAL CRIME

Knowledge Management, Intelligence Strategy and Executive Leadership

PETTER GOTTSCHALK

Reviews for Investigation and Prevention of Financial Crime

'This theoretical reference frame is an important prerequisite for enlightened discussions and reflections. This book contains important findings about methods to combat financial crime and can support police organizations and relevant authorities aiming to prevent this type of crime.'

Dr. Stefan Holgersson, Växjö University, Sweden.

'The book provides a unique insight into the practice and investigation of financially motivated crime. First a comprehensive overview of different types of financial crime in the context of knowledge management is provided, offering a unique perspective on the adoption of strategies to prevent such crime as well as investigative techniques that might be employed to combat financial criminal activity. The book will serve as a useful reference for police practitioners, those working in the criminal justice system and researchers interested in this area.'

Professor Julia C. Davidson, Director of Research in Criminology, Kingston University. UK.

Contents

List of Figures

List of Tables

Introduction

So long as there are weaknesses that can be exploited for gain, companies, other organizations and private individuals will be taken advantage of. This theoretically-based but practitioner-oriented book focuses on what is generally seen as financial or economic crime. Such profit-driven crime is categorized according to type as theft, fraud, manipulation and corruption.

Providing a source of authoritative and detailed information on understanding the methods used in all of these types of financial crime and steps that can be taken to avoid and combat it, this book addresses important topics including organized crime, money laundering, cyber crime, corruption in law enforcement agencies and whistle blowing. This book considers how, in some competitive environments, goals can seem to legitimize all kinds of means, and how culture can exert a role in relation to what is seen as acceptable or unacceptable behaviour by individuals.

An important perspective in this book is how strategies for the use of intelligence might combat financial crime, and the uniqueness in this approach lies in the way this book is able to explain intelligence and intelligence processes in the wider context of knowledge and knowledge management.

While data are numbers and letters without meaning, information is data in a context that makes sense. Information combined with interpretation, reflection and context is knowledge, while knowledge accumulated over time as learning is wisdom. In this hierarchical structure we find intelligence as more than information, while less than knowledge. Intelligence is analyzed information. Intelligence can provide the basis for opening a new criminal case, it can be applied to the investigation of existing criminal cases, it can be used to reallocate investigative resources based on new crime patterns and actors, and it can be used for preventive measures. Case studies throughout the book illustrate the investigation and prevention of financial crime from an intelligence, knowledge management and systems perspective.

Financial crime is often defined as crime against property, involving the unlawful conversion of property belonging to another to one's own personal use and benefit. Financial crime is profit-driven crime to gain access to and control over property that belonged to someone else. Pickett and Pickett (2002) define financial crime as the use of deception for illegal gain, normally involving breach of trust, and some concealment of the true nature of the activities. They use the terms financial crime, white-collar crime and fraud interchangeably.

The term financial crime expresses different concepts depending on the jurisdiction and the context. Nevertheless, Henning (2009) argues that financial crime generally describes a variety of crimes against property, involving the unlawful conversion of property belonging to another to one's own personal use and benefit, more often than not involving fraud but also bribery, corruption, money laundering, embezzlement, insider trading, tax violations, cyber attacks and the like. Criminal gain for personal benefit seems to be one of the core characteristics of financial crime.

Financial crime often involves fraud. Financial crime is carried out via cheque and credit card fraud, mortgage fraud, medical fraud, corporate fraud, bank account fraud, payment (point of sale) fraud, currency fraud and health care fraud, and they involve acts such as insider trading, tax violations, kickbacks, embezzlement, identity theft, cyber attacks, money laundering, and social engineering. Embezzlement and theft of labour union property and falsification of union records used to facilitate or conceal such larcenies remain the most frequently prosecuted Labour-Management Reporting and Disclosure Act offences in the US (Toner, 2009).

Financial crime sometimes, but not always, involves criminal acts such as elder abuse, armed robbery, burglary and even murder. Victims range from individuals to institutions, corporations, governments and entire economies.

Interpol (2009) argues that financial and high-tech crimes – currency counterfeiting, money laundering, intellectual property crime, payment card fraud, computer virus attacks and cyber-terrorism, for example – can affect all levels of society.

Michel (2008) argues that financial crime is opportunity driven. Opportunity is a flexible characteristic of financial crime and varies depending on the type of criminals involved. Types of financial crime can vary as much as the criminal organizations and criminal businessmen involved. The opportunity emerges

when a weakness in a procedure has been discovered. Opportunities appear when a risk exists.

When comparing legal and illegal activities, Michel (2008) argues that the reasons why businessmen retain the services of experts in the financial market are the same as those of criminals. The assignment will be justified for reasons of competency.

White-collar crime contains several clear components (Pickett and Pickett, 2002):

- *It is deceitful.* People involved in white-collar crime tend to cheat, lie, conceal and manipulate the truth.

- *It is intentional.* Fraud does not result from simple error or neglect but involves purposeful attempts to illegally gain an advantage. As such, it induces a course of action that is predetermined in advance by the perpetrator.

- *It breaches trust.* Business is based primarily on trust. Individual relationships and commitments are geared toward the respective responsibilities of all parties involved. Mutual trust is the glue that binds these relationships together, and it is this trust that is breached when someone tries to defraud another person or business.

- *It involves losses.* Financial crime is based on attempting to secure an illegal gain or advantage and for this to happen there must be a victim. There must also be a degree of loss or disadvantage. These losses may be written off or insured against or simply accepted. White-collar crime nonetheless constitutes a drain on national resources.

- *It may be concealed.* One feature of financial crime is that it may remain hidden indefinitely. Reality and appearance may not necessarily coincide. Therefore, every business transaction, contract, payment or agreement may be altered or suppressed to give the appearance of regularity. Spreadsheets, statements and sets of accounts cannot always be accepted at face value; this is how some frauds continue undetected for years.

- *There may be an appearance of outward respectability.* Fraud may be perpetrated by persons who appear to be respectable and professional members of society, and may even be employed by the victim.

1

Financial Crime Categories

A number of illegal activities can occur in both the commercial and public sectors. So long as there are weaknesses that can be exploited for gain, companies and other organizations as well as private individuals will be taken advantage of (Pickett and Pickett, 2002).

Therefore, we find a great variety of criminal activities that are classified as financial crime. This chapter attempts to develop main categories as well as subcategories of financial crime. The four main categories are labelled fraud, theft, manipulation and corruption respectively. Within each main category there are a number of subcategories. This chapter is based on exploratory research to stimulate future research in refining and improving the categories suggested here and illustrated in Figure 1.1.

Fraud Crime

Fraud can be defined as an intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right. Fraud is unlawful and intentional making of a misrepresentation, which causes actual prejudice or which is potentially prejudicial to another (Henning, 2009).

ADVANCE FEE FRAUD

Victims are approached by letter, faxes or e-mail without prior contact. Victims' addresses are obtained from telephone and e-mail directories, business journals, magazines and newspapers. A typical advance fraud letter describes the need to move funds out of Nigeria or some other sub-Saharan African country, usually the recovery of contractual funds, crude oil shipments or inheritance from late kings or governors (Ampratwum, 2009). This is an external kind of

fraud, where advance fee fraudsters attempt to secure a prepaid commission for an arrangement that is never actually fulfilled or work that is never done.

Victims are often naïve and greedy, or at worst prepared to abet serious criminal offences such as looting public money from a poor African state. The advance fee fraud has been around for centuries, most famously in the form of the Spanish prisoner scam (Ampratwum, 2009: 68):

> *In this, a wealthy merchant would be contacted by a stranger who was seeking help in smuggling a fictitious family member out of a Spanish jail. In exchange for funding the 'rescue' the merchant was promised a reward, which of course, never materialized.*

Advance fee fraud is expanding quickly on the Internet. Chang (2008) finds that this kind of fraud is a current epidemic that rakes in hundreds of millions of dollars per year. The advent of the Internet and proliferation of its use in the last decades makes it an attractive medium for communicating the fraud, enabling a worldwide reach. Advance fee fraudsters tend to employ specific methods that exploit the bounded rationality and automatic behaviour of victims. Methods include assertion of authority and expert power, referencing respected persons and organizations, providing partial proof of legitimacy, creating urgency, and implying scarcity and privilege.

BANK FRAUD

Fisher (2008) describes a US banking fraud case. It involved Jeffrey Brett Goodin, of Azusa, California who was sentenced to 70 months imprisonment as a result of his fraudulent activities. Goodin had sent thousands of e-mails to America Online (AOL's) users that appeared to be from AOL's billing department and prompted customers to send personal and credit card information, which he then used to make unauthorized purchases. The e-mails referred the AOL customers to one of several web pages where the victims could in-put their personal and credit information. Goodin controlled these web pages, allowing him to collect the information that enabled him and others to make unauthorized charges on the AOL users' credit or debit cards.

Bank fraud is a criminal offence of knowingly executing a scheme to defraud a financial institution. For example in China, bank fraud is expected to increase both in complexity and in quantity as criminals keep upgrading their fraud methods and techniques. Owing to the strong penal emphasis

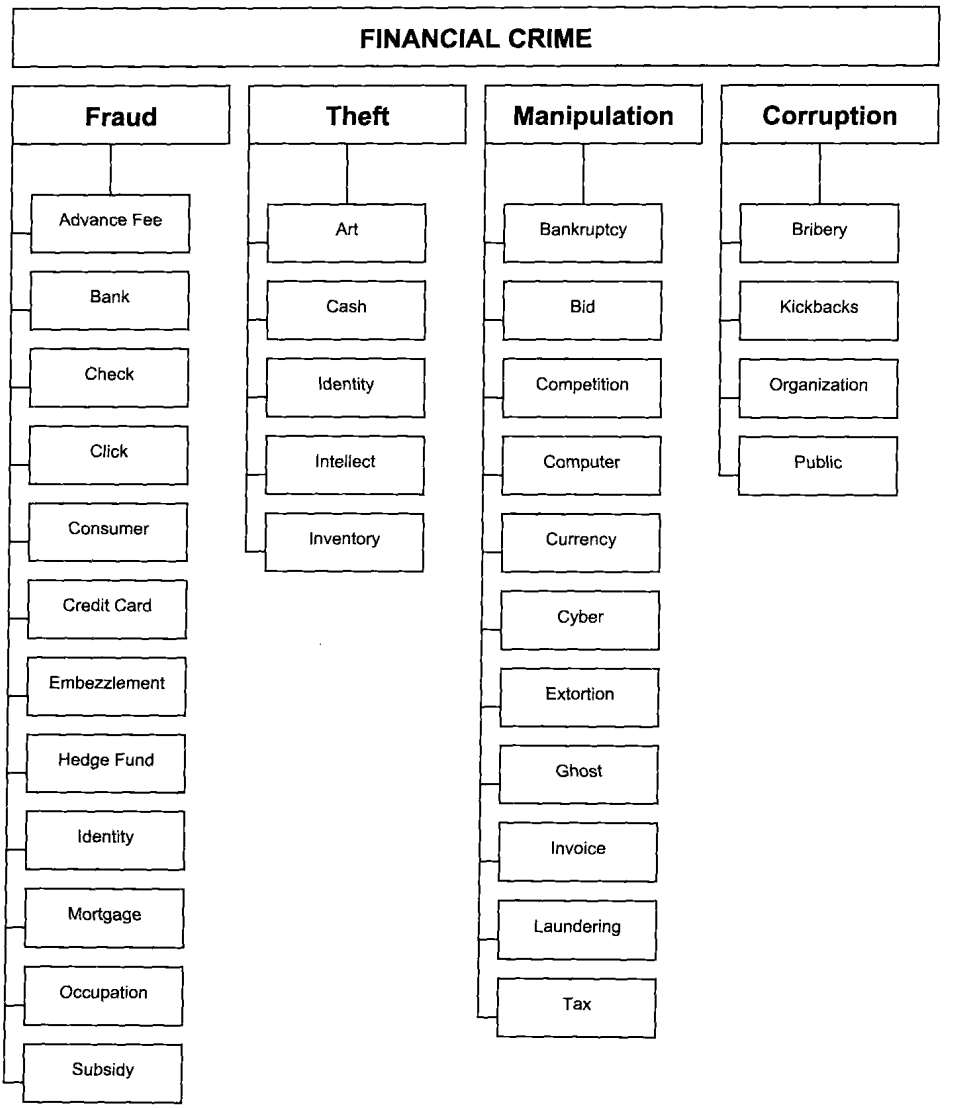

Figure 1.1 Main categories and subcategories of financial crime

of Chinese criminal law, harsh punishment including death penalty and life imprisonment has been used frequently for serious bank fraud and corruption. Cheng and Ma (2009) found, however, that the harshness of the law has not resulted in making the struggle against criminals more effective. The uncertain law and inconsistent enforcement practices have made offenders more fatalistic about the matter, simply hoping they will not be the unlucky ones to get caught.

Financial fraud in the banking sector is criminal acts often linked to financial instruments, in that investors are deceived into investing money in a financial instrument that is said to yield a high profit. Investors lose their money because no investment actually takes place, the instrument does not exist, the investment cannot produce the promised profit or it is a very high-risk investment unknown to the investor. The money is usually divided between the person who talked the investor into the deal and the various middlemen, who all played a part in the scheme (Økokrim, 2008).

CHEQUE FRAUD

When a company cheque is stolen, altered or forged, it may be diverted to an unauthorized person who accesses the funds and then closes the account or simply disappears (Pickett and Pickett, 2002).

CLICK FRAUD

This occurs when an individual or computer program fraudulently clicks on an online advertisement without any intention of learning more about the advertiser or making a purchase. When you click on an advertisement displayed by a search engine, the advertiser typically pays a fee for each click, which is supposed to direct potential buyers to its product. Click fraud has become a serious problem at Google and other websites that feature pay-per-click online advertising. Some companies hire third parties (typically from low-wage countries) to fraudulently click on a competitor's advertisements to weaken them by driving up their marketing costs. Click fraud can also be perpetrated with software programs doing the clicking.

CONSUMER FRAUD

These are attempts to coerce consumers into paying for goods not received or goods that are substandard, not as specified, or at inflated prices or fees. The growing use of Internet websites, as an alternative to unsolicited phone calls or visits to potential customers, compounds this problem (Pickett and Pickett, 2002).

Consumer fraud is a term also used in the opposite meaning, where the consumer is fraudulent. An example is consumer insurance fraud, which is defined as a deliberate deception perpetrated against an insurance company for the purpose of financial gain. Common frauds include misrepresentation of

facts on an insurance application, submission of claims for injuries or damages that never occurred, arrangement of accidents and inflation of actual claims (Lesch and Byars, 2008). Insurance fraud is a global economic problem that threatens the financial strength of insurers and threatens the survival of the insurance institutions (Yusuf and Babalola, 2009).

CREDIT CARD FRAUD

This is use of stolen credit card details to secure goods or services in the name of the cardholder. Sometimes a brand new credit card is forged using known details. Cards can be stolen or details obtained from files that are not properly secured; credit card details may also be purchased from people who are able to access this information (Pickett and Pickett, 2002). Credit card fraud can be considered a subcategory of identity theft (Gilsinan et al., 2008).

One of the worst data thefts for credit card fraud ever was carried out by 11 men in five countries (Laudon and Laudon, 2010: 326):

> In early August 2008, US federal prosecutors charged 11 men in five countries, including the US, Ukraine and China, with stealing more than 41 million credit and debit card numbers. This is now the biggest known theft of credit card numbers in history. The thieves focused on major retail chains such as OfficeMax, Barnes & Noble, BJ's Wholesale Club, the Sports Authority and T.J. Maxx.
>
> The thieves drove around and scanned the wireless networks of these retailers to identify network vulnerabilities and then installed sniffer programs obtained from overseas collaborators. The sniffer programs tapped into the retailers' networks for processing credit cards, intercepting customers' debit and credit card numbers and personal identification numbers (PINs). The thieves then sent that information to computers in the Ukraine, Latvia and the US. They sold the credit card numbers online and imprinted other stolen numbers on the magnetic stripes of blank cards so they could withdraw thousands of dollars from ATM machines. Albert Gonzales of Miami was identified as a principal organizer of the ring.
>
> The conspirators began their largest theft in July 2005, when they identified a vulnerable network at a Marshall's department store in Miami and used it to install a sniffer program on the computers of the chain's parent company, TJX. They were able to access the central TJX database, which stored customer

transactions for T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the US and Puerto Rico, and for Winners and HomeSense stores in Canada. Fifteen months later, TJX reported that the intruders had stolen records with up to 45 million credit and debit card numbers.

TJX was still using the old Wired Equivalent Privacy (WEP) encryption system, which is relatively easy for hackers to crack. Other companies had switched to the more secure Wi-Fi Protected Access (WPA) standard with more complex encryption, but TJX did not make the change. An auditor later found that TJX had also neglected to install firewalls and data encryption on many of the computers using the wireless network, and did not properly install another layer of security software it had purchased. TJX acknowledged in a Securities and Exchange Commission filing that it transmitted credit card data to banks without encryption, violating credit card company guidelines.

There are many different forms of credit card fraud. One of the more simple methods involves the unauthorized use of a lost or stolen card. Another form of credit card fraud is commonly known as non-receipt fraud. This occurs when the credit card is stolen while in transit between credit issuer and the authorized account holder. A third form involves counterfeit credit cards, which is a scheme utilizing credit card-sized plastic with account numbers and names embossed on the cards. In many instances, a counterfeit crime ring will recruit waiters and waitresses from restaurants to get the necessary information from customers through the use of skimming and apply the information from the magnetic strip or chip to the counterfeit card (Barker et al., 2008).

EMBEZZLEMENT

Embezzlement is the fraudulent appropriation to personal use or benefit of property or money entrusted by another. The actor first comes into possession of the property with the permission of the owner (Williams, 2006).

HEDGE FUND FRAUD

Hedge fund fraud may cause substantial losses for hedge fund investors. Hedge fund is defined by Muhtaseb and Yang (2008) as a pooled investment that is privately organized and administered by a professional management firm and not widely available to the public. The fund managers often invest a considerable amount of their own wealth in the funds they manage. They