POLICING FINANCIAL CRIME

POLICING FINANCIAL CRIME

INTELLIGENCE STRATEGY IMPLEMENTATION

PETTER GOTTSCHALK

BrownWalker Press
Boca Raton

Policing Financial Crime: Intelligence Strategy Implementation

BrownWalker Press
Boca Raton, Florida • USA
2009

ISBN-10: 1-59942-513-0 *(paper)*
ISBN-13: 978-1-59942-513-9 *(paper)*

ISBN-10: 1-59942-514-9 *(ebook)*
ISBN-13: 978-1-59942-514-6 *(ebook)*

www.brownwalker.com

Library of Congress Cataloging-in-Publication Data

Gottschalk, Petter, 1950-
Policing financial crime : intelligence strategy implementation / Petter Gottschalk.
p. cm.
Includes bibliographical references.
ISBN-13: 978-1-59942-513-9 (pbk. : alk. paper)
ISBN-10: 1-59942-513-0 (pbk. : alk. paper)
1. Commercial crimes. 2. Business enterprises--Corrupt practices. 3. Law enforcement. 4. Commercial crimes--Case studies. 5. Business enterprises--Corrupt practices--Case studies. I. Title.

HV6768.G686 2009
363.25'968--dc22

2009036661

CONTENTS

INTRODUCTION

In the fall of 2008, a man of West African origin was sentenced to 4 years and 6 months imprisonment by a court in Norway. He was charged with being an accomplice to the illegal smuggling and distribution of 1 kilo cocaine, and with the aggravated handling of the proceeds of crime for having exchanged approximately 2.2 million Norwegian crooner (300.000 US dollars) and transferred approximately 1.4 million Norwegian crooner (200.000 US dollars) out of the country (Norway), and with having used false ID documents (Financial Intelligence Unit, 2008).

The Financial Intelligence Unit (2008) in Norway had in this case prepared an analysis based on information from several messages (suspicious transaction reports from financial institutions in Norway) received one year before. The messages were received due to large and frequent currency exchanges and money transfers out of the country. Persons who did not appear to have legal access to the amounts of money in question conducted the currency exchanges and transfers.

The Financial Intelligence Unit (2008) reported the matter to the local police district in Norway, which prosecuted the African, and the court sentenced him to 4 years and 6 months

imprisonment. This is an example of a financial intelligence case on which this book is based.

This book is a source of authoritative and detailed information on understanding the methods used in economic crime and the steps that can be taken to avoid and combat it. Important topics include money laundering, organized crime, cyber crime and whistle blowing.

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.

Financial crime often involves fraud. Financial crime is carried out via check 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 labor union property and falsification of union records used to facilitate or conceal such larcenies remain the most frequently prosecuted Labor-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.

·I·

CATEGORIES OF FINANCIAL CRIME

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 sub categories of financial crime. The four main categories are labeled corruption, fraud, theft, and manipulation 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

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.

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 behavior 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.

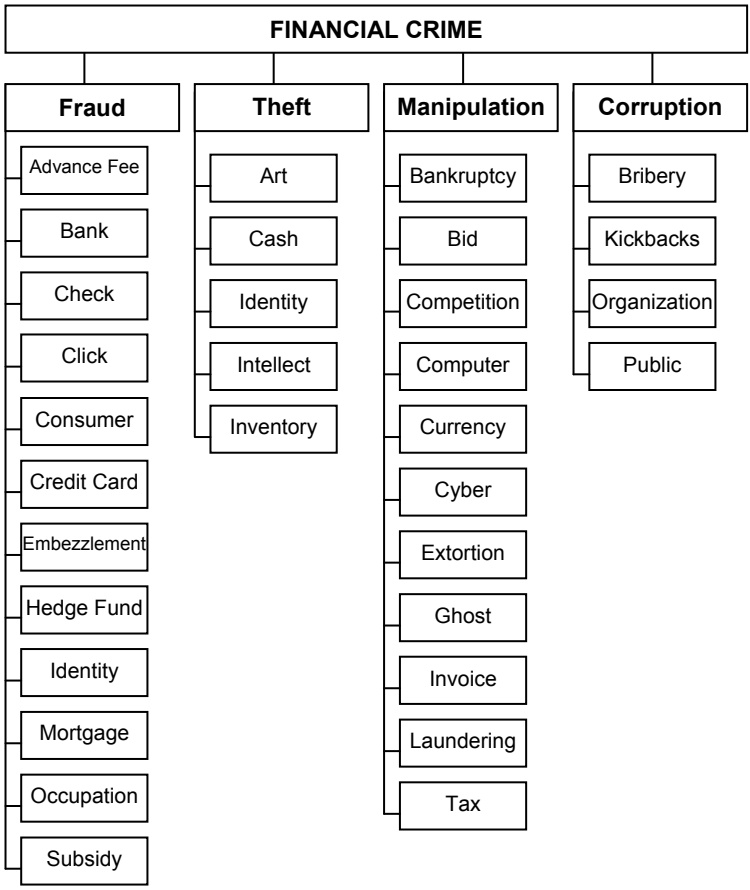

Figure 1.1. *Main categories and sub categories of financial crime*

Bank fraud is a criminal offense 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 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).

Check Fraud. When a company check 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 occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase. When you click on an ad 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 web sites that feature pay-per-click online advertising. Some companies hire third parties (typically from low-wage countries) to fraudulently click on a competitor's ads 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).

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 sub category of identity theft (Gilsinan et al., 2008).

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

> In early August 2008, U.S. federal prosecutors charged 11 men in five countries, including the United States, 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 PINs (personal identification numbers). The thieves then sent that information to computers in the Ukraine, Latvia, and the United States. 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. Marxx, Marshalls, HomeGoods, and A.J. Wright stores in the United States 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 counter-

feit 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 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 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 tend to refuse to discuss their trading strategies because they do not want competitors to imitate their moves.

Muhtaseb and Yang (2008) presented the following hedge fund fraud case. Samuel Israel, James Marquez and Daniel Marino set up and managed Bayou Funds in 1996. Marquez had a good reputation and was well connected in the industry, as he had been a former trader for the billionaire hedge fund manager George Soros. Customers invested more than $450 million in Bayou from 1996 to 2005. The leftover funds were approximately $100 million. To hide and perpetuate their fraudulent scheme, the managers knowingly misrepresented the value and performance of Bayou Funds, and issued false and misleading financial documents to investors. In 2005, Israel sent a letter to the investors that Bayou Funds would shut down at the end of the month. He said that he wanted to spend more time with his children after his divorce. Investors started asking for their money back. Israel sent another letter to explain that the process had been slowed down by auditing work because they had to make sure that the funds closed with accurate book records. The letter also stated that investors

would get 90 percent of their money back in the following week and the rest of capital a little later. However, none of the investors ever received a single penny back. The truth was revealed by Marino's suicide note typed on six pages late 2005.

Identity Fraud. There are many reported cases where people have had to defend themselves against claims, because others have stolen their identity, using personal data such as social security number, address, and date of birth (Pickett and Pickett, 2002).

Identity fraud is based on identity theft that is a crime in which an imposter obtains key pieces of personal information, such as social security identification numbers, driver's license numbers, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials (Laudon and Laudon, 2010).

Mortgage Fraud. To obtain a mortgage for real estate acquisition by a private person, the person has to state his or her income. Before the financial crisis in 2008 in the US, it was determined that 60 percent of the applicants for the loans examined overstated their income by 50 percent or more (Linn, 2009). Often, borrowers and real estate professionals combined to engage in fraud for profit schemes. Such schemes exploited the defining characteristics of sub prime lending such as 100 percent financing and weak underwriting standards. In an industry driven by commissions, lending officers were encouraged to participate in fraud schemes. The more loans the lenders' sales representatives could originate, the more money they made. Mortgage brokers and individuals inside lending institutions thus had powerful incentives to join mortgage fraud schemes by adding dirt to the loan files. They were staging loan files to include false documents as well as ignoring obvious misrepresentations on loan documents.

Occupational Fraud. Most developed countries have experienced a number of occupational fraud cases in the last decade, including the Enron, WorldCom, Societe Generale, and the Parmalat frauds. Peltier-Rivest (2009) defines occupational

fraud as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. Any fraud committed by an employee, a manager or executive, or by the owner of an organization where the victim is the organization itself may be considered occupational fraud, which is sometimes called internal fraud. Sometimes labeled financial statement fraud, inaccurate earnings figures may be used as a basis for performance bonuses (Pickett and Pickett, 2002).

Included in occupational fraud is basic company fraud. For example, when an employee fakes sickness to obtain paid sick leave, submits inflated overtime claims, or uses company equipment for an unauthorized purpose, which may be to operate a private business (Pickett and Pickett, 2002).

Peltier-Rivest (2009) studied characteristics of organizations that are victims of occupational fraud. The most frequent category of fraud in their study in Canada was asset misappropriations (81 percent of cases), followed by corruption (35 percent), and fraudulent statements (10 percent). Asset misappropriations may be cash or non-cash. Cash schemes include cash larceny, skimming, or fraudulent disbursements such as billing schemes, payroll fraud, check tampering, and expense reimbursement frauds. Non-cash schemes include theft of inventory, equipment, proprietary information, and securities.

The most frequent victims of occupational fraud in the Peltier-Rivest (2009) study were private companies, followed by government entities, and public companies. The mean loss suffered by private companies was one million US dollars. The study was based on a sample of 90 complete cases of occupational fraud investigated in Canada.

The same definition of occupational fraud is used by the Association of Certified Fraud Examiners in the USA (ACFE, 2008): Occupational fraud is the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. The association argues that the typical organization loses 7% of its annual revenues to occupational fraud.

Subsidy Crime pertains to criminal offences committed when government subsidies are granted. A person or a business might provide incorrect information when applying for government subsidies, or use the subsidies contrary to intentions and agreements (Økokrim, 2008). A similar kind of fraud of the public is sundry frauds, where an example is illegal price fixing cartels (Pickett and Pickett, 2002).

Theft

Theft can be defined as the illegal taking of another person's, group's or organization's property without the victim's consent.

Art Theft is art crime involving theft by burglary, robbery, deception (frauds, fakes, forgery, and false attribution), and might involve money laundering. Hill (2008) suggests that the monetary value of stolen works of art is not as great as the value of art frauds, fakes, forgeries, dodgy attributions and bogus provenance in the art, antiques and antiquities world.

One kind of art theft is trophy art crime, where some violent criminals enjoy the self-esteem, self-regard and self-indulgence they feel when committing high profile art crimes at specific times, often when police resources are stretched. Some examples include (Hill, 2008: 445):

1. The theft of the original version of Edvard Munch's 'Scream', stolen from the National Gallery in Oslo on the first day of the 1994 Winter Olympics in Lillehammer.
2. The theft of a portrait attributed to Rembrandt, called 'Rembrandt's Mother', from Wilton House, Wiltshire on Bonfire Night, November 5, 1994.
3. The theft of Titian's 'Rest on the Flight into Egypt' and two other sixteenth century pictures from Longleat House, Wiltshire on Twelfth Night, January 6, 1995.
4. The theft of the Ashmolean's only Cezanne in Oxford on Millennium Eve night 2000.
5. The armed robbery at the Isabella Stewart Gardner Museum in Boston, Massachusetts on the night of St. Patrick's Day 1990 in which several Rembrandts, a Vermeer and other highly significant works of art were stolen.

The financial value of stolen art varies, as the market for such stolen goods is limited. Hill (2008) argues that money laundering through works of art is serious, but more a matter of tax evasion, rather than from the laundering of illicit drug profits.

Bowman (2008) argues that trafficking in antiques is a crime of transnational proportions because it involves the illegal removal and export of cultural material from source countries, which supplies the demand, generated from developed, rich, market economies. Transnational crime against culture includes looting at archaeological sites and the grey market in antiquities on a global scale.

Theft of Cash. For example, skimming occurs when cash is taken before it enters the books. Embezzlement involves direct breach of trust, when someone entrusted with the cash diverts it for personal use. Lapping is a technique whereby the theft of cash or checks is covered up by using later receipts so that the gap in funds is not noticed (Pickett and Pickett, 2002).

Identity Theft, often combined with identity fraud, is the unlawful use of another's personal identifying information. It involves financial or other personal information stolen with intent of establishing another person's identity as the thief's own. It occurs when someone uses personally identifying information, like name, social security number, date of birth, government passport number, or credit card number without the owners' permission, to commit fraud or other crimes (Higgins et al., 2008).

Higgins et al. (2008) argue that identity theft is a behavior that threatens the growth and development of economies worldwide and has been viewed as the crime of the new millennium. In their study, they found that states with more males, higher residential mobility, and more entertainment establishments are likely to have more identity theft complaints.

Intellectual Property Crime. Intellectual property crime is a serious financial concern for car manufacturers, luxury goods makers, media firms and drug companies. Most alarmingly according to Interpol (2009), is that counterfeiting endangers

public health, especially in developing countries, where the World Health Organization estimates more than 60 percent of pharmaceuticals are fake goods.

Interpol (2009) launched a new database on international intellectual property crime, which was created to fill the void in seizure data collated by various international bodies and the private sector. Of 1,710 entities in the database, checks against other Interpol databases revealed links to credit card and currency counterfeiting, fraud, money laundering, theft, violent crimes and trafficking in human beings, weapons and drugs. This demonstrates the role of organized crime in large-scale counterfeiting and piracy.

Intellectual property's rising value in the production of wealth has been mirrored by its increasing vulnerability to crime. Snyder and Crescenzi (2009) found that intellectual property crime is often linked to cyber crime, and they explored the risks of crime inherent in intellectual capital and a distributed cyber environment to demonstrate that traditional legal remedies are largely ineffective to protect property rights.

Inventory Theft. This is stealing from a company (Pickett and Pickett, 2002).

Manipulation

Manipulation can be defined as a means of gaining illegal control or influence over others' activities, means and results.

Bankruptcy Crime is criminal acts committed in connection with bankruptcy or liquidation proceedings. A person filing for bankruptcy or a business that has gone into liquidation can hide assets after proceedings have been initiated, thereby preventing creditors from collecting their claims. However, most of the criminal acts are typically committed before bankruptcy/liquidation proceedings are initiated, e.g. the debtor has failed to keep accounts or has unlawfully withdrawn money from the business (Økokrim, 2008).

Bid Rigging. When a vendor is given an unfair advantage to defeat an open competition for a given contract. A vendor may be provided with extra information to bid low but then raise

more income through many variations to the set contract. This may be linked to the receipt of kickbacks (Pickett and Pickett, 2002).

Competition crime is collaborating on and influencing prices, profits and discounts as well as tender and market sharing collaboration. The prohibition regulations in competition laws first of all target cartel collaboration where market participants in a particular industry collaborate in order to limit the competition. They may divide the market between themselves and agree what prices to charge their customers. Prices will be higher than if real competition prevailed in the market (Økokrim, 2008).

Computer Crime is defined as any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution (Laudon and Laudon, 2010). The initial role of information and communication technology was to improve the efficiency and effectiveness of organizations. However, the quest of efficiency and effectiveness serves more obscure goals as fraudsters exploit the electronic dimension for personal profits. Computer crime is an overwhelming problem that has brought an array of new crime types (Picard, 2009). Examples of computer-related crimes include sabotage, software piracy, and stealing personal data (Pickett and Pickett, 2002).

In computer crime terminology, the term cracker is typically used to denote a hacker with a criminal intent. No one knows the magnitude of the computer crime problem – how many systems are invaded, how many people engage in the practice, or the total economic damage. According to Laudon and Laudon (2010), the most economically damaging kinds of computer crime are denial-of-service attacks, where customer orders might be rerouted to another supplier.

Counterfeit Currency. Currency counterfeiting and money laundering have the potential to destabilize national economies and threaten global security, as these activities are sometimes used by terrorists and other dangerous criminals to finance their activities or conceal their profits (Interpol, 2009). The