Categories of financial crime

Petter Gottschalk
Norwegian School of Management, Oslo, Norway

Abstract

Purpose – The purpose of this paper is to present a systematic approach to classify financial crime into main categories as well as sub categories.

Design/methodology/approach – Based on a literature review, the main four categories were labeled corruption, fraud, theft, and manipulation, respectively.

Findings – There is a massive variety of crime types and crime names in the literature that can successfully be allocated to main categories of financial crime.

Research limitations/implications – The paper is based on exploratory research to stimulate future research in refining and improving the categories suggested here.

Practical implications – The great variety of criminal activities is classified in this paper so that practitioners can organize their thinking around crime themes rather than crime examples when mapping crime.

Social implications – The public and society at large will be able to understand the confusing variety of financial crime in terms of main categories.

Originality/value – There has been some confusion among both researchers and practitioners when communicating about examples of financial crime. The organizing framework in this paper will help allocate crime examples to main categories of financial crime.

Keywords Corruption, Fraud, Theft, Classification

Paper type Research paper

Introduction

In the fall of 2008, a man of West African origin was sentenced to four years and six 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 (POC) for having exchanged approximately 2.2 million Norwegian kroner (US $300,000) and transferred approximately 1.4 million Norwegian kroner (US $200,000) out of the country (Norway), and also having used false ID documents.

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. The currency exchanges and transfers were conducted by persons who did not appear to have legal access to the amounts of money in question.

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 four years and six months imprisonment.

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

Journal of Financial Crime
Vol. 17 No. 4, 2010
pp. 441-458

1359-0790
DOI 10.1108/13590791011082797

of the true nature of the activities. They use the terms financial crime, white-collar crime, and fraud interchangeably. 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.

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 USA (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.

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).

As this introduction has illustrated, financial crime comes in all kinds of shapes and colors. No obvious categorization or classification of financial crime has emerged in the literature so far. There is a need for classification into categories of financial crime, because categories enable a structure within which policing and law enforcement can work. Therefore, this paper suggests a structure of main categories and subcategories as shown in Figure 1. The main categories in the figure are described in this paper.

Corruption

Corruption is defined as the giving, requesting, receiving, or accepting of an improper advantage related to a position, office, or assignment. The improper advantage does not have to be connected to a specific action or to not-doing this action. It will be sufficient if the advantage can be linked to a person's position, office, or assignment (Økokrim, 2008). An individual or group is guilty of corruption if they accept money or money's worth for doing something that he is under a duty to do anyway, that he is under a duty not to do, or to exercise a legitimate discretion for improper reason (Ksenia, 2008). Corruption is to destroy or pervert the integrity or fidelity of a person in his discharge of duty, it is to induce to act dishonestly or unfaithfully, it is to make venal, and it is to bribe.

Corruption involves behavior on the part of officials in the public or private sectors, in which they improperly and unlawfully enrich themselves and/or those close to them, or induce others to do so, by misusing the position in which they are placed. Corruption covers a wide range of illegal activity such as kickbacks, embezzlement, and extortion.

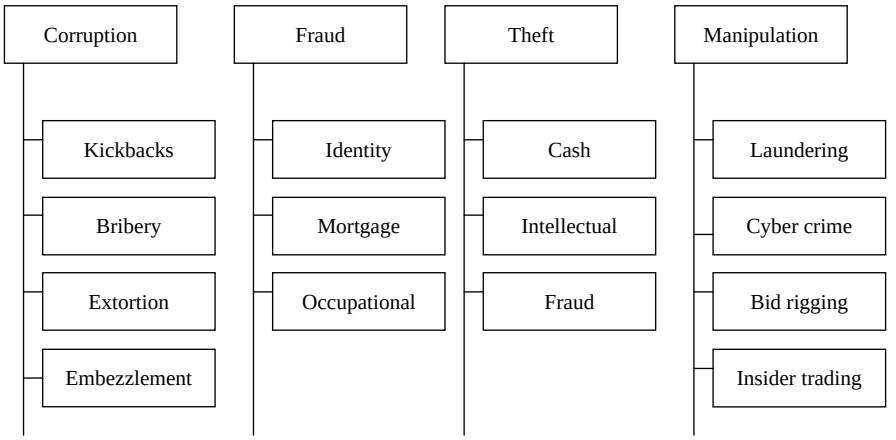

Figure 1.
Main categories and sub categories of financial crime

Kayrak (2008) includes money laundering as well in his definition of corruption. The notion of corruption may be classified as sporadic or systemic corruption, bureaucratic or political corruption, grand or petty corruption, and active and passive corruption.

Bowman and Gilligan (2008) suggest that corruption may be a greater issue for the Australian public than has been assumed in the past, given the relatively low levels of reported systematic corruption in Australia. Moreover, while there may be widespread agreement that corruption in Australia is harmful and perhaps inevitable, people can find it difficult at times to differentiate between what is corrupt and what is not.

Kickbacks

An employee with influence over who gets a particular contract is able and willing to obtain something for assisting the prospective contractor. Likewise, bribes may be paid to inspectors to turn a blind eye to substandard goods coming into a loading dock. If bribes do not work, the dedicated fraudster may well turn to blackmail and pose threats (Pickett and Pickett, 2002).

Modern criminal justice systems try to ensure that victims of crime are compensated for injuries and losses suffered at the hands of the defendant. Therefore, Young (2009) phrased the question: does the same apply to victims of corruption? The crime of corruption tends to be unique, and gains and losses involved can be substantial. The proceeds of corruption, if traceable, are often in another jurisdiction thereby complicating recovery. For example, when 11 Siemens executives were prosecuted in Germany for briberies all over the world, the victims in terms of competitors and customers could not easily be identified and compensated.

Public corruption is the abuse of entrusted power by political leaders for private gain. The corrosive effect of corruption undermines all efforts to improve governance and foster development. Corruption is just as much an economic problem as it is a political and social one, since it is a "cancer" that burdens the poor in developing countries (Berkman *et al.*, 2008, p. 125):

> Corruption works to undermine development projects in three primary ways. First, the world's poor often do not receive the full benefit of development aid because as much as 10, 20, 30 and even higher percentages of development loans are siphoned off – often in the form of bribes – by corrupt actors, such as government officials, contractors, and in rare cases, by employees of international organizations. Bribe payers in turn short-change the project by, for example, using substandard materials or performing below specification, in order to pay these bribes.
>
> Second, even though aid recipients may consequently receive only a fraction in benefits from every dollar or euro spent for development aid because of corruption, they nonetheless have to pay back the full amount of the development loan, often with interest. The resulting debt burdens placed on the world's poor stifle any chance they may have of freeing themselves from the vexing cycle of poverty and debt. Worse still, the poor in developing nations grow cynical of international organizations that lend money to corrupt leaders while providing little or no oversight to ensure these loans are used for the purposes intended.
>
> Third, corruption leads to donor fatigue. Taxpayers from donor countries, along with their elected representatives responsible for approving development aid budgets, are increasingly skeptical that development projects are being effectively implemented. Pleas from international aid agencies that more aid is needed for development projects or famine relief are increasingly falling on the deaf ears of taxpayers, who perceive that international organizations either ignore, or do little to stop, the corruption that makes a mockery of international aid.

Public corruption is found all over the world. Sato (2009) tells the story about Pacific Consultants International (PCI), a Japanese consulting firm, which had paid an $820,000 bribe to a Ho Chi Minh City official. In a highway construction project in Vietnam, PCI made the payment as a reward for helping secure a consultancy service contract of $3 million.

Corruption can play an important role in the building up of criminal organizations. Criminal entrepreneurs may expand their illegal activities by bribing local officials. An example can be found in Brazil, where the Rabelo brothers built up their criminal enterprise by corrupting a reliable network of alliances. The Rabelo enterprise is in the cocaine business, and they have built up reliable relationships within political elites. When studying the Rabelo enterprise, Filho (2008) found that organized crime in Brazil could grow quickly because of the absence of an effective judicial system, the lack of social service delivery by the government as well as cultural factors.

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.

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 web sites, 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 11 men in five countries (Laudon and Laudon, 2010, p. 326):

In early August 2008, US 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. Marxx.

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 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).

External fraud

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

Inventory theft

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

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).

Araujo (2009) developed a model to study an incentive-based approach to fraud prevention in companies. The theory of incentives was applied to design a mechanism that makes employees reveal their true type, that is, their willingness or ability to combat corruption. The mechanism design approach used in the study assumes that the manger or the principal is entrusted with the power of making the employees agents.

Click fraud
This 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.

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).

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).

Financial statement fraud
Inaccurate earnings figures may be used as a basis for performance bonuses (Pickett and Pickett, 2002).

Sundry frauds
An example is illegal price fixing cartels (Pickett and Pickett, 2002).

Embezzlement
This 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).

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 USA, 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 subprime 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.

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.

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.

Peltier-Rivest (2009) study describes and explains 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 percent of it annual revenues to occupational fraud.

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).

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, p. 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.

Financial fraud

This is criminal acts 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 loose 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).

Subsidy crime

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).

Hedge fund fraud

This 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) present 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.

Theft

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).

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.

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.

Identity theft

This 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).

Identity theft 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.

Art theft

This 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, p. 445):

- The theft of the original version of Edvard Much's "Scream", stolen from the National Gallery in Oslo on the first day of the 1994 Winter Olympics in Lillehammer.
- The theft of a portrait attributed to Rembrandt, called "Rembrandt's Mother", from Wilton House, Wiltshire on Bonfire Night, November 5, 1994.
- 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.
- The theft of the Ashmolean's only Cezanne in Oxford on Millennium Eve night 2000.
- 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.

Manipulation

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).

Inflated invoices
A company inflates its bills without agreement from the bill payer, who may be a customer. Conversely, an employee may arrange to pay a vendor more than is due in return for an unauthorized payment or some other gain (Pickett and Pickett, 2002).

Boyrie *et al.* (2007) studied capital movement through trade misinvoicing. Data from 30 African nations were examined for deviations from average import and export prices as an indicator of capital flow. The results of the study demonstrated that capital outflow from African nations to the USA grew my more than 50 percent from 2000 to 2005.

Travel and entertainment (subsistence) claims
This is when claims are falsified, inflated, or there is basic abuse of the schemes (Pickett and Pickett, 2002).

Ghost employees
This is getting extra names onto a company payroll and diverting the funds to a bank account specifically set up for this scam. If an employee can stay on the payroll after having left the company, again extra funds can be obtained for a while (Pickett and Pickett, 2002).

Misappropriation schemes
Altering sales figures, writing off income that was actually received, obtaining blank purchase orders, amending documentation, diverting vendor discounts, and writing off balances are some examples here (Pickett and Pickett, 2002).

Computer-related crimes
Examples include sabotage, software piracy, and stealing personal data (Pickett and Pickett, 2002).

Extortion
For the first time in a published decision in the USA, the Court of Appeals approved the reach of the federal extortion statute to the operation of employee pension and health plans (Toner, 2009, p. 49):

> In the *Gotti* case the organized criminal defendants were convicted of having obtained by extortion health plan participants' intangible right to have their plan trustees and fiduciaries contract with pharmaceutical and mental health service providers of their choice and discharge their duties in the best interest of the plan. The organized crime defendants were convicted of plotting to have the health plan trustees award these contracts to mob favored companies; especially one ran by an individual who had paid substantial monies to a mob leader for support in getting a prescription drug contract.

In another court case in the USA, extortion victims were prosecuted (Ferrer, 2009). It started in 1997 when Carlos Castaño, Head of Autodefensas Unidas Campesinas (AUC), a Colombian paramilitary group, met with the general manager of the Colombian subsidiary of Chiquita, a major banana-exporting corporation. In that meeting, Castaño informed Chiquita that the AUC was engaged in military operations in the area. Castaño sent an "unspoken but clear message" that failure to make payments to the AUC in exchange for its "protection" could result in physical harm to Chiquita's personnel and property. Chiquita paid almost $2 million to the AUC. However, the US secretary of state

had designated the AUC as a terrorist organization. Chiquita, a US corporation operating in Colombia and confronted with threats of life and property loss, was found liable for making illicit payments to the AUC.

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 crime of counterfeiting currency is as old as money itself. In the past, nations had used counterfeiting as a means of warfare. The idea was to overflow the enemy's economy with fake banknotes, so that the real value of the said money was reduced, and thereby attacking the economy and general welfare of a society.

Income tax crime

The failure to comply with national income tax laws is one of the most prevalent financial crimes in many countries. The Internal Revenue Service in the USA estimated that 245 billion dollars represents the total individual tax gap in the nation (Cecil *et al.*, 2009). Tax evasion can be divided into three main categories (Økokrim, 2008): undeclared work/business, unlawful planning and adjustment of taxes, and exploitation of ambiguities or alleged "loopholes" in the legislation so as to obtain improper tax advantages.

Malkawi and Haloush (2008) distinguished between tax avoidance and tax evasion. Tax avoidance is the act of taking advantage of legally available opportunities to minimize one's tax liability. Individuals and legal entities tend to choose a tax alternative which will incur the least income tax liability. This is known as tax planning that is taking place within certain legal boundaries. However, tax planning strategies encounter boundaries that are sometimes difficult to identify. For example, there is a gray area between tax avoidance, which is legal tax saving, and tax evasion, which is illegal.

Tax evasion is defined as the willful attempt to defeat or circumvent the tax law in order to illegally reduce one's tax liability. Tax evasion is illegal while tax avoidance is a legal approach to saving taxes. In many legislation regions, the crime of tax evasion requires a positive action. A mere passive neglect of the statutory duty is then insufficient to establish violation. Acts such as submitting incorrect statements of accounts, making false entries or alterations, or false books or records, destruction of books and records, concealment of assets, or covering up sources of income constitute tax evasion (Malkawi and Haloush, 2008).

Compliance and ethics in taxation was studied by Ho and Wong (2008). They found that ethical beliefs could be an effective means to improve tax compliance, particularly for taxpayers with lower levels of moral development. Also, as tax compliance rate is found to be higher when taxpayers have a stronger moral belief that tax evasion is not ethical, a stronger enforcement effort might have a positive overall effect on tax compliance.

A special kind of tax fraud is value-added tax (VAT) fraud. Pashev (2007) studied cross border VAT fraud in terms of credit mechanisms known as missing trader or carousel fraud.

Cyber crime

Attacks on the cyber security infrastructure of business organizations can have several goals. One goal pursued by criminals is to gain unauthorized access to the target's sensitive information. Most businesses are vitally dependent on their proprietary information, including new product information, employment records, price lists, and sales figures. According to Gallaher *et al.* (2008), an attacker may derive direct economic benefits from gaining access to and/or selling such information or may inflict damage on an organization by impacting upon it. Once access has been attained, attackers cannot only extract and use or sell confidential information, they can also modify or delete sensitive information, resulting in significant consequences for their targets.

Computer crime

This 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).

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.

Cyber crime and computer crime are both related to internet crime. The internet is a "double-edged sword" that provides many opportunities for individuals and organizations to develop. At the same time, the internet has brought with it new opportunities to commit crime. Salifu (2008) argues that internet crime has become a global issue that requires full cooperation and participation of both developing and developed countries at the international level.

Bankruptcy crime

This 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).

Competition crime

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).

Money laundering

This is an important activity for most criminal activity (Abramova, 2007; Council, 2007; Elvins, 2003). Money laundering means the securing of the proceeds of a criminal act. The proceeds must be integrated into the legal economy before the perpetrators can use it. The purpose of laundering is to make it appear as if the proceeds were acquired legally, as well as disguises its illegal origins (Financial Intelligence Unit, 2008). Money laundering takes place within all types of profit-motivated crime, such as embezzlement, fraud, misappropriation, corruption, robbery, distribution of narcotic drugs, and trafficking in human beings (Økokrim, 2008).

Money laundering has often been characterized as a three-stage process that requires:

(1) moving the funds from direct association with the crime;

(2) disguising the trail to foil pursuit; and

(3) making them available to the criminal once again with their occupational and geographic origins hidden from view.

The first stage is the most risky one for the criminals, since money from crime is introduced into the financial system. Stage 1 is often called the placement stage. Stage 2 is often called the layering stage, in which money is moved in order to disguise or remove direct links to the offence committed. The money may be channeled through several transactions, which could involve a number of accounts, financial institutions, companies, and funs as well as the use of professionals such as lawyers, brokers, and consultants as intermediaries. Stage 3 is often called the integration stage, where a legitimate basis for asset origin has been created. The money is made available to the criminal and can be used freely for private consumption, luxury purchases, real estate investment, or investment in legal businesses.

According to Joyce (2005), criminal money is frequently removed from the country in which the crime occurred to be cycled through the international payment system to obscure any audit trail. The third stage of money laundering is done in different ways. For example, a credit card might be issued by offshore banks, casino "winning" can be cashed out, capital gains on option, and stock trading might occur, and real estate sale might cause profit.

The proceeds of criminal acts could be generated from organized crime such as drug trafficking, people smuggling, people trafficking, proceeds from robberies or money acquired by embezzlement, tax evasion, fraud, abuse of company structures, insider trading, or corruption. Financial Intelligence Unit (2008) argues that most criminal acts are motivated by profit. When crime generates significant proceeds, the perpetrators need to find a way to control the assets without attracting attention to them selves or the offence committed. Thus, the money laundering process is decisive in order to enjoy the proceeds without arousing suspicion.

The POC find their ways into different sectors of the economy. A survey in Canada indicates that deposit institutions are the single largest recipient, having being identified in 114 of the 149 POC cases (Schneider, 2004). While the insurance sector was implicated in almost 65 percent of all cases, in the vast majority the offender did not explicitly seek out the insurance sector as a laundering device. Instead, because motor vehicles, homes, companies, and marine vessels were purchased with the POC, it was often necessary to purchase insurance for these assets.

References

Abramova, I. (2007), "The funding of traditional organized crime in Russia", *Economic Affairs*, Vol. 27, pp. 18-21.

ACFE (2008), *Report to the Nation – On Occupational Fraud and Abuse*, Association of Certified Fraud Examiners, Austin, TX.

Ampratwum, E.F. (2009), "Advance fee fraud '419' and investor confidence in the economies of sub-Saharan African (SSA)", *Journal of Financial Crime*, Vol. 16 No. 1, pp. 67-79.

Araujo, R.A. (2009), "Are labor contracts efficient to combat fraud?", *Journal of Financial Crime*, Vol. 16 No. 3, pp. 255-61.

Barker, K.J., D'Amato, J. and Sheridon, P. (2008), "Credit card fraud: awareness and prevention", *Journal of Financial Crime*, Vol. 15 No. 4, pp. 398-410.

Berkman, S., Boswell, N.Z., Brüner, F.H., Gough, M., McCormick, J.T., Pedersen, P.E., Ugaz, J. and Zimmermann, S. (2008), "The fight against corruption: international organizations at a cross-roads", *Journal of Financial Crime*, Vol. 15 No. 2, pp. 124-54.

Bowman, B.A. (2008), "Transnational crimes against culture: looting at archaeological sites and the 'Grey' market in antiquities", *Journal of Contemporary Criminal Justice*, Vol. 24 No. 3, pp. 225-42.

Bowman, D. and Gilligan, G. (2008), "Public awareness of corruption in Australia", *Journal of Financial Crime*, Vol. 14 No. 4, pp. 438-52.

Boyrie, M.E., Nelson, J.A. and Pak, S.J. (2007), "Capital movement through trade misinvoicing: the case of Africa", *Journal of Financial Crime*, Vol. 14 No. 4, pp. 474-89.

Cecil, H.W., Placid, R.L. and Pacini, C. (2009), "Income tax crime and government responses in the United States 1998-2007", *Journal of Financial Crime*, Vol. 16 No. 1, pp. 97-106.

Chang, J.J.S. (2008), "An analysis of advance fee fraud on the internet", *Journal of Financial Crime*, Vol. 15 No. 1, pp. 71-81.

Cheng, H. and Ma, L. (2009), "White collar crime and the criminal justice system – government response to bank fraud and corruption in China", *Journal of Financial Crime*, Vol. 16 No. 2, pp. 166-79.

Council (2007), *Council Conclusions Setting the EU Priorities for the Fight Against Organized Crime Based on the 2007 Organized Crime Threat Assessment*, Council of the European Union, Brussels.

Elvins, M. (2003), "Europe's response to transnational organised crime", in Edwards, A. and Gill, P. (Eds), *Crime: Perspectives on Global Security*, Routledge, London, pp. 29-41.

Ferrer, M. (2009), "Prosecuting extortion victims: how counter-terrorist finance measure executive order 13224 is going to far", *Journal of Financial Crime*, Vol. 16 No. 3, pp. 262-88.

Filho, L.A. (2008), "The dynamics of drug-related organized crime and corruption in Brazil from a development perspective", *Journal of Financial Crime*, Vol. 15 No. 1, pp. 49-59.

Financial Intelligence Unit (2008), Annual Report, Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim), Oslo.

Fisher, J. (2008), "The UK's faster payment project: avoiding a bonanza for cybercrime fraudsters", *Journal of Financial Crime*, Vol. 15 No. 2, pp. 155-64.

Gallaher, M.P., Link, A.N. and Rowe, B.R. (2008), *Cyber Security – Economic Strategies and Public Policy Alternatives*, Edward Elgar, Cheltenham.

Gilsinan, J.F., Millar, J., Seitz, N., Fisher, J., Harshman, E., Islam, M. and Yeager, F. (2008), "The role of private sector organizations in the control and policing of serious financial crime and abuse", *Journal of Financial Crime*, Vol. 15 No. 2, pp. 111-23.

Higgins, G.E., Hughes, T., Ricketts, M.L. and Wolfe, S.E. (2008), "Identity theft complaints: exploring the state-level correlates", *Journal of Financial Crime*, Vol. 15 No. 3, pp. 295-307.

Hill, C. (2008), "Art crime and the wealth of nations", *Journal of Financial Crime*, Vol. 15 No. 4, pp. 444-8.

Ho, D. and Wong, B. (2008), "Issues on compliance and ethics in taxation: what do we know?", *Journal of Financial Crime*, Vol. 15 No. 4, pp. 369-82.

Interpol (2009), *Financial and High-tech Crimes*, International Criminal Police Organizaton (Interpol), Lyon, available at: http://interpol.int/Public/FinancialCrime/Default.asp (accessed 3 July 2009).

Joyce, E. (2005), "Expanding the international regime on money laundering in response to transnational organized crime, terrorism, and corruption", in Reichel, P. (Ed.), *Handbook of Transnational Crime and Justice*, Sage, London, pp. 79-97.

Kayrak, M. (2008), "Evolving challenges for supreme audit institutions in struggling with corruption", *Journal of Financial Crime*, Vol. 15 No. 1, pp. 60-70.

Ksenia, G. (2008), "Can corruption and economic crime be controlled in developing countries and if so, is it cost-effective?", *Journal of Financial Crime*, Vol. 15 No. 2, pp. 223-33.

Laudon, K.C. and Laudon, J.P. (2010), *Management Information Systems: Managing the Digital Firm*, 11th ed., Pearson Education, London.

Lesch, W.C. and Byars, B. (2008), "Consumer insurance fraud in the US property-casualty industry", *Journal of Financial Crime*, Vol. 15 No. 4, pp. 411-31.

Linn, C.J. (2009), "The way we live now: the case for mandating fraud reporting by persons involved in real estate closings and settlements", *Journal of Financial Crime*, Vol. 16 No. 1, pp. 7-27.

Malkawi, B.H. and Haloush, H.A. (2008), "The case of income tax evasion in Jordan: symptoms and solutions", *Journal of Financial Crime*, Vol. 15 No. 3, pp. 282-94.

Michel, P. (2008), "Financial crimes: the constant challenge of seeking effective prevention solutions", *Journal of Financial Crime*, Vol. 15 No. 4, pp. 383-97.

Muhtaseb, M.R. and Yang, C.C. (2008), "Portraits of five hedge fund fraud cases", *Journal of Financial Crime*, Vol. 15 No. 2, pp. 179-213.

Økokrim (2008), Annual Report 2007, Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime, Oslo.

Pashev, K.V. (2007), "Countering cross-border VAT fraud: the Bulgarian experience", *Journal of Financial Crime*, Vol. 14 No. 4, pp. 490-501.

Peltier-Rivest, D. (2009), "An analysis of the victims of occupational fraud: a Canadian perspective", *Journal of Financial Crime*, Vol. 16 No. 1, pp. 60-6.

Picard, M. (2009), "Financial services in trouble: the electronic dimension", *Journal of Financial Crime*, Vol. 16 No. 2, pp. 180-92.

Pickett, K.H.S. and Pickett, J.M. (2002), *Financial Crime Investigation and Control*, Wiley, New York, NY.

Salifu, A. (2008), "The impact of internet crime on development", *Journal of Financial Crime*, Vol. 15 No. 4, pp. 432-43.

Sato, Y. (2009), "How to deal with corruption in transitional and developing economies – a Vietnamese case study", *Journal of Financial Crime*, Vol. 16 No. 3, pp. 220-8.

Schneider, S. (2004), "Organized crime, money laundering, and the real estate market in Canada", *Journal of Property Research*, Vol. 21 No. 2, pp. 99-118.

Snyder, H. and Crescenzi, A. (2009), "Intellectual capital and economic espionage: new crimes and new protections", *Journal of Financial Crime*, Vol. 16 No. 3, pp. 245-54.

Toner, G.A. (2009), "New ways of thinking about old crimes: prosecuting corruption and organized criminal groups engaged in labor-management racketeering", *Journal of Financial Crime*, Vol. 16 No. 1, pp. 41-59.

Williams, H.E. (2006), *Investigating White-Collar Crime: Embezzlement and Financial Fraud*, Charles C. Thomas, Springfield, IL.

Young, S.N.M. (2009), "Why civil actions against corruption?", *Journal of Financial Crime*, Vol. 16 No. 2, pp. 144-59.

Further reading

Chang, J.J., Lu, H.C. and Chen, M. (2005), "Organized crime or individual crime? Endogenous size of a criminal organization and the optimal law enforcement", *Economic Inquiry*, Vol. 43 No. 3, pp. 661-75.

Corresponding author

Petter Gottschalk can be contacted at: petter.gottschalk@bi.no