Int. Journal of
Financial Technology Perspective (FinTech)
Vol.2, No.5, Summer 2025

Fintech Forensics: Opportunities And Challenges

Seyed MohammadJafar Mirzapour Ale Hashem
Ph.D. Candidate of Accounting, Faculty of Economics and Management, Islamic Azad University Science and Research Branch, Tehran, Iran.
(Corresponding author)
Behyad_65@yahoo.com

Alireza khojasteh
Ph.D. Candidate of Accounting, Faculty of Economics and Management, Islamic Azad University Science and Research Branch, Tehran, Iran.

Submit: 02/05/2023 Accept: 03/07/2023

Abstract

In recent decades, with the introduction of digital technologies into our daily lives, our lifestyles have completely changed, and the field of finance and accounting is no exception to this rule, which resulted in the formation of a field called financial technology. This paper describes an emerging subdiscsipline of digital forensics which covers financial technologies. The digital transformation of society is introducing new financial technologies, or Fintech, for payments, funds transfer, and other financial transactions. Criminals are leveraging financial technologies for fraud ,extortion, money laundering, and financing activity in the criminal under ground. The type of financial crimes has changed from the traditional to the modern way, which has led to the formation of an emerging discipline called fintech forensics, which through the use of new technologies help preventing and detecting all types of financial frauds and organized financial crimes, like money laundering, underground economic activities, Financial Corporation and etc.

Keywords

Fintech, cyber-crime, cyber fraud, underground economy, phishing, crypto currency, money laundering.

1. Introduction

In our days, all digital devices such as cell phones, tablets, laptops and desktop computers can be used for criminal activities such as fraud, drug trafficking, homicide, hacking, forgery, terrorism, etc. To fight against these criminal activities Fintech forensics is used to help investigate cybercrimes and to identify the device-assisted crime (Chaturvedi et al, 2019). Cyber forensics is the application of examination and analysis techniques to gather and preserve evidence from an appropriate computing device in a way that is suitable for presentation in a court of law. The goal of cyber forensics is to perform a careful investigation while maintaining a documented chain of evidence to find out exactly what to be found on a computing device and who was blamed for it. Digital Forensics tools are now used on a daily basis by examiners and analysts.

The research aspect of Fintech forensics is also discussed, including both theoretical and applied research. Areas of further research are described, and the collaboration between the finance industry and academia is highlighted to foster academic research. The paper concludes with thoughts on the future evolution of financially motivated crime and Fintech forensics. Currently there is a gap to be filled between traditional fraud investigators and traditional digital forensic investigators. Traditional fraud investigators have a comprehensive knowledge of payment systems and money flows, but often have limited technical knowledge of the underlying systems. Conversely, traditional digital forensics investigators have a comprehensive knowledge of underlying technical systems, but often lack knowledge of financial transaction activity. Recognizing Fintech Forensics as a knowledge domain will close this gap and provide researchers and practitioners with technical knowledge of Fintech systems combined with financial knowledge of payment systems. This will help society fight crime more effectively when financial technologies are involved (Nikkel, 2020).

2. Emerging & Developing of Fintech Forensics

Forensic Accounting and Fraud Investigation provides an up-to-date resource for detecting, preventing, and successfully prosecuting financial fraud. It addresses all phases of forensic accounting, complete with actual examples demonstrating application in the real world. It provides non-experts with access to all the critical accounting principles and investigative techniques that help protect any organization from fraud, including insightful advice on where an organization is most susceptible to fraud and how to implement effective investigation processes when fraud is suspected. Ask any two practicing forensic accountants to define what forensic accounting is, and you are likely to get two different answers. Both may be accurate, and there likely will be some similarities within the responses, but still there is no one consistent answer recited by everyone who practices in this specialized area of accounting. The responses provided will depend largely on the background, experience, and areas of practice of each individual forensic accountant. Forensic accounting definitions commonly refer to fraud, fraud prevention, and fraud investigations as the role of the forensic accountant. While those definitions are not necessarily inaccurate, they provide a definition of forensic accounting only within the specific context of fraud. They continue in discussions about forensics and accounting to include a much longer but equally understandable definition, as follows (Pedneault & etc, 2012):

"Forensic accounting is the action of identifying, recording, settling, extracting, sorting, reporting, and verifying past financial data or other accounting activities for settling current or prospective legal disputes or using such past financial data for projecting future financial data to settle legal disputes."

The digital transformation of society is introducing new financial technologies, or Fintech, for payments, funds transfer, and other financial transactions.

Criminals are leveraging financial technologies for fraud, extortion, money laundering, and financing activity in the criminal underground. The investigation of Fintech and digital payment activity needs to be recognized as a new technical sub-discipline of the digital forensics landscape. The digital forensics community is well positioned to provide research for practitioners to enhance investigations involving Fintech and technical financial activity. The word Fintech often invokes thoughts of startup companies or new technologies hoping to become the "Uber" equivalent for banks. But the definition of Fintech goes beyond startups and covers a broad range of technologies for conducting financial activities (Nikkel, 2020). While a number of Fintech definitions exist, one methodically researched definition states Fintech is a new financial industry that applies technology to improve financial activities (Schueffel, 2016).

Here researched a number of proposed "Fintech" definitions and consolidated them to create a broader definition. Traditional banks cannot be excluded from the definition of Fintech. On the contrary, banks are actively developing new digital payment systems and technical financial products. Blockchain based virtual or crypto currencies can also be considered as an alternative financial technology. Bitcoin has captured public attention, but many others exist, for example: Ethereum, Monero, and Litecoin. These are included as financial technologies in this paper, even though the financial industry and regulatory bodies are still hesitant to accept them as legitimate forms of currency. These new financial systems are moving towards digital wallets which allow simple online payment for parking, vending machines, transportation, and other common purchases. They facilitate the direct transfer of money between individuals, allow monthly payments for traditional services, and replace the need for cash in traditional stores (Nikkel, 2020).

The commonly accepted definition of digital forensic science comes from DFRWS (2001):

"*Digital Forensic Science: The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*."

By combining the definitions of Fintech and digital forensics, a basic definition of Fintech forensics (which includes the context of cyber-criminal activity) can be defined as:

"Fintech Forensics: The application of digital forensic science to financial technologies for the purpose of investigating and reconstructing criminal financial activity".

The discipline of digital forensics encompasses many different areas including computer forensics, network forensics, mobile forensics, malware forensics, IoT forensics, drone and vehicle forensics, and so on. This paper argues for the addition of Fintech forensics to this landscape of digital forensic research and practitioner expertise. The rest of this paper describes examples to help set the scope of Fintech forensics and the context in which it is used. Also included is a discussion of Fintech Forensic researchers and practitioners (Nikkel, 2020).

Scenarios requiring Fintech Forensics

To illustrate the concept of Fintech forensics, a number of real world example incidents involving financial technologies are presented. Here the benefit of technical forensic analysis of financial activity is shown. Europol's IOCTA report provides a useful overview of current criminal activity, including crimes using and abusing financial technologies (Europol, 2020). Fraud refers to the unlawful appropriation of

property, including money. Cyber fraud refers to committing fraud over the Internet, in particular, the online theft of money. Cyber fraud investigations involve the reconstruction of financial transactions and money flows between multiple parties. Typical cyber-criminal activity involves financial transactions between the following groups (Nikkel, 2020):

- victims to criminals (theft or extortion of funds),
- criminals to criminals (purchases and payments in the criminal underground),
- criminals to financial institutions (money laundering)
- The investigation of cyber fraud and other technical manipulation of financial systems typically involves understanding and reconstructing.

criminal activity, attribution of people or organizations involved in the crime, and finally the collection and preservation of digital evidence. A comprehensive technical understanding of financial technologies will enhance each of these phases. This technical analysis must support or align with existing investigative activities, for example forensic accounting and auditing, AML investigations, and traditional fraud and crime investigations. Fintech forensic investigation and analysis should not compete with these longstanding areas, but rather complement and strengthen them. Internet or Cyber fraud is already included in standard fraud taxonomies alongside traditional wire fraud and mail fraud (Beals et al.,2015).

Types of Fintech Forensics

In this Internet era, more and more frauds will be perpetrated using computers and networks. Whether the potential fraudster is a disgruntled employee, greedy executive, or unethical business partner, there are many opportunities to defraud a company or organization. Pressure, opportunity, and rationalization are the three elements of every fraud. Investigators should look for evidence of each of these factors—and not focus solely on opportunity. In order to prove fraud, the prosecutor must show intent and deceit. E-mail and other electronic communication media often contain evidence of deceit and intent as well as pressures or rationalization for stealing from a company (Chaturvedi et al, 2019). According to the research findings of Nikkel (2020) and Faccia et al (2019) studies, some of the types of Fintech Forensics are:

Phishing methods for committing financial fraud

Classic phishing involves sending emails to large numbers of people with links to a webpage impersonating a bank. The webpage then requests login credentials or credit card details. Access to online bank accounts lead to stolen funds, and stolen credit cards are monetized. Smishing, or SMS phishing, involves sending victims a text message impersonating a financial institution. The message may contain a link to a classic phishing page or include a phone number. In either case a victim is approached and the end result is financial fraud. Vishing, or Voice phishing, involves criminals contacting victims by phone and impersonating bank staff. Plausibility is increased when combined with local languages and accents, and other social engineering tactics. Vishing attacks use VoIP extensively to hide or impersonate calls.

Twishing, or Twitter phishing, and other social media phishing involves criminals using social media platforms for targeting victims. This may include the creation of account names that look similar to a financial institution, impersonating bank executives, or sending messages claiming to be bank staff. Victims are then contacted and together with further social engineering, fraud is committed.

In all of these phishing variants, technical methods are used to contact victims and commit fraud. Fintech forensics in these scenarios would involve understanding the entire chain of the fraud attack, from the initial contact to the final transfer of funds. Digital evidence is collected from each step of the attack, and investigations to determine attribution are made.

Attacks against ATMs and payment card terminals

There are also some crimes involving financial technologies which are not necessarily conducted over the Internet but still have a technological aspect. Automatic Teller Machines (ATMs) are frequently targeted to steal magnetic card strip data as the card is inserted into the ATM. Skimming refers to an electronic device placed over the card insertion slot which reads the magnetic strip. A separate camera is placed with a view of the keypad to intercept the PIN. The PIN and card information are collected by criminals (physically or using wireless remote access) and then used for fraud.

Shimming refers a thin electronic device placed inside the card insertion slot, allowing the card data to be intercepted, and placing a man-in-the-middle between the card's chip and chip reader. ATMs have a regular PC inside them, controlling the dispensing of cash. Some attacks involve compromising this PC (via USB or other means) to cause "Jack-potting", which causes the machine to dispense large amounts of cash. A more advanced attack involves compromising the central control systems which manage the ATM or payment card terminal networks. When criminals gain control of these central systems, they are able to dispense cash and steal financial information at a larger scale.In these examples, either hardware is manipulated or systems are compromised leading to the theft of cash or information. Fintech forensics in these scenarios would involve analysis of the hardware and compromised ATM or payment card terminal to determine how access to systems and information was gained, and how the attack was monetized.

Online banking trojans (PC and mobile)

Online banking malware, or banking trojans, involve infecting computers leading to unauthorized access of bank accounts to make fraudulent payments. The computer becomes part of a criminal network of infected machines called a botnet. When any user tries to access their online banking portal the malware becomes active, manipulating the session to prepare fraudulent payments. Once a bank account is successfully emptied, the malware will prevent further logins or manipulate the user interface to avoid detection.

Mobile banking malware is a growing concern in the finance industry. This involves infecting mobile phones to target existing payment apps. The most common method is an overlay attack, where the finger taps are intercepted and manipulated and a modified screen output is presented back to the user. When a mobile banking app is used, the malware takes control of the interaction between the person and the apps to commit fraudulent payment activity. The interception of SMS based authentication (MTANs) is also common with mobile malware. In both these scenarios phishing or smishing is typically used to deliver malware to the user and infect the device. Fintech forensics in this context would involve understanding how the malware is interacting with the banking applications and creating payments. In addition, various anomalies of the fraudulent payment can be analyzed, and the transfer of stolen funds to a money mule can be further investigated.

Rogue mobile banking apps

Rogue mobile banking apps involve criminals writing apps and submitting them to mobile app stores. As these apps are legitimate programs, not malware, they are difficult to detect. The apps will typically impersonate existing financial institutions, or claim to be a financial service. Users install the app and are prompted for passcodes and credit card details which are then monetized or used for fraud. In this scenario, Fintech forensics would refer to the detailed forensic analysis of the app functionality, what information is stolen, and how that information is used to commit fraud.

Extortion and ransom attacks

The recent growth in extortion and ransom attacks does not directly involve the finance industry, but still constitutes financial fraud by extortion. DDoS for Bitcoin, or "DD4BC" involves criminals emailing an organization threatening to use a distributed denial of service attack to disable the companies Internet

infrastructure. A short demonstration of DDoS attack capability is executed, followed by an email demanding funds in crypto currencies in order to prevent further attacks. Ransomware involves the compromise of a company's infrastructure to encrypt files and data (including backups). Once data is encrypted, the company is offered the decryption keys after a payment in crypto currency is received. More recent ransom attacks exfiltrate company internal data and demand money to prevent public disclosure. Sextortion attacks target individuals via email, claiming to have infected the victim's PC and making embarrassing videos with the webcam. The criminals threaten to make the video public or send it to family and friends unless money is sent to a crypto currency wallet. Recent variations of this attack involve claims of a hired hitman to cause death or physical harm to the victim, unless money is paid to prevent it. In these scenarios, Fintech forensics would include the analysis of the initial contact, but focus heavily on the transfer of funds to crypto currencies. In situations where contact with fraudsters can be established, further investigation may be possible and eventually lead to attribution and recovery of stolen funds.

Online social engineering attacks to commit fraud

The most common and well-known social engineering attacks are phone calls claiming to be “Microsoft Support”. Victims are led to believe their computers have technical problems and after a long phone call of fake support, credit card payment is demanded. In some cases, remote access software is also installed to covertly monitor and manipulate the victim's PC, including the hijacking of online banking sessions to make fraudulent payments. More advanced attacks involve criminals using open source intelligence to research3 a victim organization prior to the attack. Criminals claiming to be a vendor or partner of the company contact a chosen employee who is able to make financial transactions.

The amount of internal knowledge about the company increases plausibility and trust, allowing the criminal to socially manipulate the victim into executing a fraudulent payment on backend systems.The Fintech forensic analysis in these scenarios involves the analysis of the entire attack including the financial movement of money, but in particular the technical exploitation involved in transferring the funds.

BEC and CEO impersonation

Social engineering attacks via email are increasing, and when combined with carefully selected business targets can result in significant fraud losses. Business Email Compromise, or BEC, involves unauthorized access to business email accounts for the purpose of sending impersonated payment requests or manipulating invoices to other businesses. Passwords to business mail accounts are phished or otherwise acquired and criminals are able to login as the account owner. The criminals search for previous invoices or payment requests, and re-use them to communicate instructions for fraudulent funds transfers or payments. Since the criminal is logged in as the legitimate user, it is difficult to notice the sender is not legitimate.

Another popular form of email based social engineering is known as CEO impersonation fraud. This involves the creation of a free email account using the name (firstname-lastname@) of a senior executive at a targeted company. Social engineered emails impersonating the manager are sent to carefully selected employees instructing them to execute fraudulent payments.

In both these scenarios the fraudulent payments tend to be high amounts which are common in a business finance context. The fintech analysis here analyzes the entire chain from first contact until final funds transfer. Attempts can be made to link technical traces found in the communication (email headers for example) with technical information from the destination bank for the purpose of fraudster attribution.

Compromised payment processing infrastructure

The most lucrative method used to steal money from a financial institution is to compromise core banking systems. The SWIFT payment network connects financial institutions to allow funds transfer messages

between banks. When criminals compromise trusted bank internal SWIFT infrastructure they have the ability to arbitrarily transfer funds to any destination. The most well known SWIFT attack was against a Bangladesh bank (Shevchenko, 2016).

Many countries also have regional payment processing networks that can be targeted. Another new risk (yet to be fully exploited by criminals) is the proliferation of payment aggregators. These are small companies (often startups) who write apps or platforms that interface with multiple banks to provide a single unified interface. This involves trusting the aggregator company with direct access to all the person's bank accounts and authorizes payment activity on behalf of the user. In Europe the PSD2[European Union, 2015] regulation specifically allows such services which use APIs to submit payment instructions. These companies may become prime targets in the future, as they bypass the usual user interface to the bank where anomaly detection is typically done.

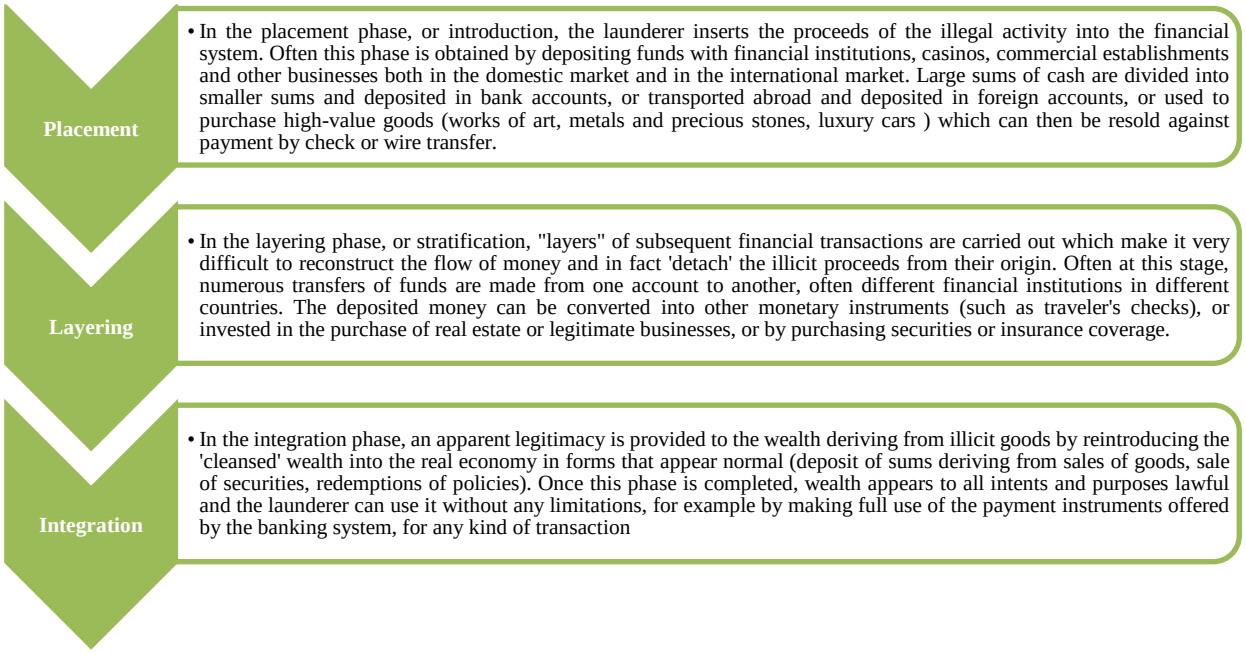
A further type of attack involves compromising the internal financial applications of medium sized companies. These platforms are managed by the company's finance departments and have an established trusted interface to banks for the purpose of making payments and performing other corporate banking activities. Some malware is designed to compromise the users of these back-office finance systems, creating fraudulent payments which appear to be legitimate business.The fintech analysis here requires extensive knowledge of technical payment interfaces between banks, businesses, and payment processing organizations. These are technically complex attacks involving malware, intrusions, and compromised or manipulated messaging protocols. A Fintech forensic analysis would reconstruct the entire attack from beginning to end, and include analysis of the destination bank accounts used to receive the fraudulent funds.

Money Laundering

Three key points that refer to concrete cases that emerged in the recent past. Crypt currency exchanges take place on unregulated platforms and numerous cases of thefts have occurred without users being able to protect their rights. On the subject of money laundering, the non-traceability of Crypt currencies has made it possible to move suspicious assets which ended up in the sights of the authorities. The exchange channel allows to bypass authorized financial intermediaries and transactions are not safe (Faccia et al ,2019). With a specific reference to Money Laundering, Money it takes place:

a. in the classic case of “washing” of the money (i.e. the elimination of any possible connection with the previous offense (replacement conduct),
b. in the transfer, through negotiation tools, of goods of illicit origin (transfer conduct),
c. in carrying out other operations aimed at hindering the identification of the criminal origin of the goods, considered as a closing clause aimed at pursuing conduct not previously identified by the legislator and which are the result of the “creativity” with which the criminal groups work to recycle the dirty money.

Therefore, the anonymity of crypt currencies along with a lack of control by a centralized authority represents an appealing opportunity for money laundering and, in general, for the reinvestment of capital of illegal origin. Although money laundering is often the result of a complex series of transactions, it is always the result of three distinct steps (Schneider & Windischbauer, 2008): Placement, Layering and Integration.



Steps of Money Laundering
(Resource: Faccia et al ,2019)

Online money laundering

When funds are stolen, criminals employ money mules to hide their tracks and launder the money. In some cases people, hoping to get part-time jobs as “financial intermediaries”, are hired as mules through online job portals or through spam campaigns (“earn extra money in your spare time!”). When money is stolen, it is transferred to the mule's account and they are expected to withdraw cash, keep an agreed portion, and forward the rest to another recipient (typically using a cash transfer service).

For large amounts, criminals can't rely on private people hired from public sources or forums. Professional mules (MaaS - Mules as a Service) can be hired in the criminal underground. They are more expensive but they are reliable and can be trusted with large amounts of stolen funds. These mules typically appear as companies, not individuals.

A growing method of laundering money with anonymity is the use of crypto currencies. Some crypto currencies like bitcoin have a transparent blockchain which reveals all transactions. There exist systems called “tumblers” or“mixers” which mix the Bitcoins with other funds in an attempt to obfuscate the link between source and destination. Other crypto currencies are designed with anonymity built into their blockchain. Since crypto currencies are decentralized and unregulated, they can be used without knowing the identities of the sender or receiver. The Fintech forensic analysis aspect of money laundering covers the online mule recruitment process, the mechanisms used to transfer stolen funds, and the analysis of the payment destination(s). Of growing importance within the sub discipline of Fintech forensics is the ability to analyze crypto currencies used by criminals.

EU anti-money laundering legal framework

The anti-money laundering legislation is contained in a structured system of sources at international, EU and national level. The EU rules on the prevention and

countering of money laundering and terrorist financing have, over time, incorporated the evolution of international principles, with the aim of creating a harmonized regulatory environment among Member States. The European Union's anti-money laundering commitment dates back to the early 1990s and it has been reflected, over two decades, in five Directives and several other provisions. Finally, directive no. 2018/843 of the European Parliament and of the Council of 30 May 2018 (so-called 5th Anti-Money Laundering Directive), amends the Directive no. 2015/849 (4th Anti-Money Laundering Directive). Until the 5th Directive, service providers whose business consists in the provision of exchange services between virtual currencies and legal tender currencies, and digital portfolio service providers were not subject to the Union obligation to identify and report suspicious activity (Haffke et al, 2019).

This flaw in the system has meant that terrorist groups have repeatedly handled huge financial flows in total anonymity, concealing transfers with exchanges between virtual currencies. Hence the need to modify and expand the scope of application of Directive 2015/849, so as to include these exchange service providers and digital wallet in the list of subjects obliged to pay money laundering obligations (Faccia et al , 2019).

Criminal financing in the underground economy

Criminals also buy and sell goods and services from/to other criminals. Today this is most often done using various crypto currencies, with the products and services available on darknet or underground online forums. From a cyber-crime perspective, criminals are also able to purchase much of their infrastructure and services from other criminals ("Crime-as-a-Service" model). Some examples include:

1. operating illegal online web sites and forums (bullet-proof hosting),
2. providing reliable spam campaigns to distribute emails with malicious web links or attachments,
3. renting of multipurpose botnets (large numbers of infected devices which are centrally controlled by a criminal actor),
4. selling or renting phishing kits to steal credentials for identity theft,
5. selling or renting online banking trojans for unauthorized access to bank accounts to make fraudulent payments,
6. underground alternatives to VirusTotal (but malware samples not shared).

Financial transactions among criminals are not only related to cyber fraud activity. They are also used for purchasing illegal goods and services, and financing other criminal activity. For example:

7. physical contraband such as drugs or weapons,
8. illegal material (pictures/videos) involving child sexual exploitation or extreme violence,
9. human trafficking or terrorist financing.

In the above scenarios a variety of financial technologies can be used to facilitate funds transfer. In some cases, they use services offered by the financial industry, in other cases they use open decentralized technologies like crypto currencies. In both cases, they require the technical analysis of the transfer of some form of value to/from a criminal party. This is another example of Fintech forensic analysis.

The Dark Web

Through the so-called "Dark Web" money is bought in Bitcoin, at one tenth of the value. Funds from bank accounts or online victims of violations (for example the theft of credentials associated with credit cards or payment methods) are transferred to the buyer's current account, also through the Western Union network. In return, the seller requests a payment in Bit coin for an amount equal to 10-12% of the amount sent. In the darkest parts of the Net, illegal exchange markets, packages of 2,500, 5,000 or 10,000 dollars are available. In this way, cybercriminals do not have to deal with the obligation to "wash" the money before being able to use it, shifting the responsibility to those who (at their own risk) decide to buy dirty money at about a tenth of its value. It is certainly not the first time that Bitcoin and other crypto currencies that make

it almost impossible to trace the real identity of both counterparts of the transactions used for illegal activities (Weber & Kruisbergen, 2019).

Crypto Capital Corporation

In October 2019, Polish police arrested Ivan Manuel Molina Lee, president of Crypto Capital Corporation (CCC), the company that has previously provided banking services for Bitfinex and other major trading platforms on international money laundering charges. of crypto currencies including Binance, Kraken and BitMEX[1]. Thanks to a joint operation (Europol, Interpol, Poles and US services) Molina Lee, a Canadian citizen, was extradited to Warsaw where he was wanted for laundering of 1.5 billion zlotys, about 350 million euros, obtained from illegal sources. According to the Polish allegations reported by RMF 24, Molina Lee carried out "money laundering for Colombian drug cartels using crypto currency exchange companies[2]. The law enforcement operation led by the Polish authorities is the largest in the country's history. Polish prosecutors stated that Crypto Capital Corporation held bank accounts in the small rural bank "Bank Spółdzielczy" in the city of Skierniewice and laundered illegal proceeds in the country through crypto currency exchange firm BitFinex. In recent months, Molina Lee's activities through Crypto Capital Corporation and its other affiliate, Global Trading Solutions, had been directly involved in a sort of "shadow banking system" that provided bank accounts to crypto currency companies (Faccia et al , 2019).

Coin Ninja

In February 2020, the U.S. federal government has arrested Larry Harmon, CEO of the Coin Ninja media platform and founder of the Drop Bit crypto currency wallet[3]. In particular, the man was accused of conducting money laundering activities and running a business for the exchange of funds without a specific license from FinCEN. According to the arrest warrant filed in early February, Harmon would have laundered over 354,468 Bitcoin (BTC), equivalent to approximately $ 311 million at the time of the transaction, allowing users of Helix and Grams, respectively, a privacy and privacy tool, a dark web search engine, to transact on AlphaBay, a very popular dark market but closed in 2017. For these crimes, Harmon will face a prison sentence of thirty years (Faccia et al , 2019).

Bestmixer.io

In February 2020, the Dutch tax authorities and the Fiscal Intelligence and Investigation Services (FIOD) arrested two men for allegedly laundering millions of euros in crypto currency. According to a joint statement from the Joint Chiefs of Global Tax Enforcement (J5). The FIOD arrested 2 Dutch citizens in separate investigations into tax evasion. Recovering around 260,000 in unnamed crypto currencies and over 6.6 pounds of gold. Credit and debit cards in possession of crypto currency and euros were also seized, one of the suspects using the, already banned, bitcoin mixing service Bestmixer.io. FIOD recently stepped up its crypto currency activities. Working with tax authorities in the UK, US, Australia and Canada - collectively, J5 Agents - they have been sharing tips and data since 2018. One of the biggest data dumps came shortly after FIOD seized and closed Bestmixer.io''[4].

Wirecard

Since June 2020, in Germany, a serious financial scandal involving the online payment company

1 Reference: https://www.bloomberg.com/news/articles/2019-10-25/crypto-capital-official-nabbed-in-polish-money-laundering-probe,

2 Reference:https://www.rmf24.pl/fakty/polska/news-narkotykowy-boss-wyladowal-w-warszawie-molina-lee-byl-poszuk,nId,3297567,

3 Reference:https://news.bloomberglaw.com/us-law-week/bitcoin-deemed-money-under-d-c-financial-services-law,

4 Reference: https://www.bloomberg.com/news/articles/2020-08-06/wirecard-implosion-tears-through-european-banks-bottom-lines

Wirecard is underway, after the discovery of a shortfall of 1.9 billion euros which was thought to be deposited as trust funds in two banks in the Philippines but which never existed. The former Wirecard's CEO has been arrested in Germany on suspicion of fraud, while his former CEO has disappeared after fleeing the country[5]. In addition to this fraud, according to the Financial Times[6]. Wirecard processed payments for a Maltese online casino which was later accused of laundering money for a powerful member of the 'Ndrangheta, one of Europe's most dangerous mafia organizations. Wirecard processed payments for CenturionBet, a Malta-based gaming company that was later found by Italian courts to be an 'Ndrangheta way for moving money out of the country in a sophisticated money laundering operation. Wirecard continued to trade with CenturionBet, which was incorporated in Malta but owned by a Panamanian company, until 2017 when its gambling license was suspended by the Maltese authorities and ceased trading after an anti-mafia raid that saw the arrest of 68 people.Since then over 30 people have been convicted of mafia-related crimes. CenturionBet's revenues included only a fraction of Wirecard's global operations, but the discovery raises further questions about the German company's business model, once deemed to be a pioneer of European fintech. As a regulated payment institution, Wirecard is required to abide by the strict anti-money laundering rules and report suspicious transactions to the competent authorities. Wirecard also processed payments for another larger Maltese gambling company that has been investigated by the Italian authorities for money laundering for organized crime groups. It is possible that Wirecard was unaware of the company's alleged ties to organized crime.

5 Reference:https://www.bloomberg.com/news/articles/2020-08-06/wirecard-implosion-tears-through-european-banks-bottom-lines

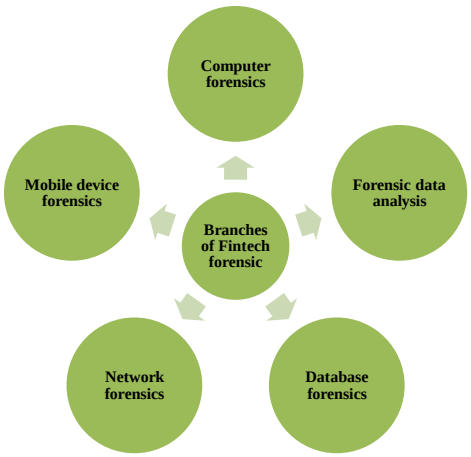
6 Reference:https://www.ft.com/content/b3eb9a37-ed8a-4218-9064-685b181740f0

Fintech forensic practitioners and researchers

The first sections of this paper developed a definition and provided context around Fintech forensics. This next section describes the people involved, in particular, the practitioners and researchers.

Branches of Fintech forensic

In general, Five main branches of Fintech forensics presented in figure (1):



Five main branches of Fintech forensics
(Resorce: Chaturvedi et al, 2019)

- **Computer Forensics and Digital Detective Work:** *Computer forensics* is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media. We all know that that the widespread use of computers and the Internet have contributed to traditional and computer crimes (Garber Lee, 2012). Effective forensic investigation of these offenses requires evidence gathered from computers, storage media, digital devices, e-mail, chat rooms, and the Internet—and any technology that tracks what was done, who did it, and when. Law enforcement and other

investigators will produce, during the discovery process, imaged or exact copies of the digital media being investigated. These copies need to be examined by trained professionals to ensure that the media have been secured and examined in the correct manner and all evidence has been recovered. There are numerous legal and ethical issues of evidence seizure, handling, and investigation. Updated and new federal rules and laws regulate forensic investigations,

- **Data, PDA, and Cell Phone Forensics:** The basic media types and devices that you will encounter when doing a forensic examination. You are most likely to encounter magnetic media devices such as hard drives and optical media devices such as CDs, but electronic devices such as USB drives are becoming more prevalent. Your job as a forensic investigator may also require you to know about data from PDAs and cellular phones (Greg Gogolin, 2013). After learning how data is stored in these various types of devices, you learned specific methods for acquiring data from each category. Some guidelines for data acquisition are the same for any device, such as the importance of making at least two copies of the data so that you can work on one copy while safeguarding the original copy and the suspect's device. Other guidelines are specific to a device, such as the importance of maintaining power to a PDA to avoid data loss. A number of suppliers such as Guidance, Paraben, AccessData, and Logicube have developed tools for capturing and analyzing data. Some of these tools are designed to work with a specific type of data, such as that acquired from PDAs, while others can be used for several different types of data,
- **Operating Systems and Data Transmission Basics for Digital Investigations:** The operating system of a computer is the program that controls the basic functions of a computer and acts as the intermediary between the application programs and hardware of a computer. The two types of interfaces used to communicate with an operating system are command line interface (CLI) and graphical user interface (GUI). The CLI interface consists of a text-based interface where commands are entered via a prompt. A GUI interface usually consists of a pointing device such as a mouse being used to interface with graphical objects, such as icons or menus, on a monitor. The functions basic to an operating system are file management, memory management, job management, device management, and security management. Early computers did not need an operating system because applications handled all computer functions. Modern computers have many applications and thus require a centralized operating system to handle applications and system information. DOS, Windows, UNIX/Linux, and Macintosh OS X are all examples of operating systems used on modern computer systems. File systems manage the basic unit of data storage called a file. Various file systems in use include FAT 16, FAT 32, NTFS, efs, UFS, and OS X. The OSI model standardized the methods used to transmit data on a network. The OSI model consists of a seven-layer approach. While the OSI model is the theoretical model to follow, the TCP/IP model is the de facto standard of the Internet. The TCP/IP model consists of a four-layer approach. The two address schemes used to transmit data across networks are logical addressing and physical addressing. Logical addressing usually consists of IP addressing, and physical addressing consists of media access control addressing,
- **Internet and Network Forensics and Intrusion Detection:** This area of computer forensics is just beginning to expand to the point where the technology is robust and reliable enough to be accepted in a court of law. Additionally, the sheer power to collect

wide ranges of data from networks is now well within the computational and storage power of most organizations. This factor, coupled with the fact that NFAT systems can enable an organization to deal in real time with internal and external network threats and to recreate what happened for future use, make this type of software extremely versatile. This chapter only covered the surface possibilities and uses for the forensic use of such software. More and more organizations will eventually move to this forensic model because it uses the power of the network to accomplish forensic tasks that at present are done in a more labor intensive and costly way.

Existing practitioner communities

A community of practitioners investigating and analyzing technical fraud already exists in the finance industry. This community emerged out of necessity over the past 10e15 years with the advancement of online banking trojans, phishing attacks, social engineering and other cyber-criminal activity targeting the finance industry (and their clients). Bank internal technical teams have been established to manage this growing risk to the bank's client segment. Criminals targeting the finance industry typically don't target one bank at a time, but often target multiple banks simultaneously. This behavior has led to more collaboration and joint response from the finance industry and law enforcement. The community today consists largely of the following groups:

- banks with a large retail client segment,
- credit card companies and issuers,
- law enforcement investigators specializing in Internet/Cyber fraud investigations,
- governmental CERTs responsible for national critical infrastructure (finance sector),
- some regions have also developed FinCERTs to manage finance sector specific security issues,
- security companies specializing in cyber fraud analysis and incident management,
- non-profit organizations collaborating with banks to fight cyber fraud,
- banking and payment associations responsible for combating fraud,
- product and solution vendors focused on banking client protection.

The management of incidents involving financial technologies is typically led by the owners of the systems being abused, i.e. the banks themselves. They will engage other players in the community for support, intelligence information exchange, and investigative collaboration. This community of practitioners has developed an extensive set of tools and techniques in response to the growing problem of cyber fraud attacks involving financial technologies. One of the goals of this paper is to bring this finance industry community closer to the digital forensics community. There is considerable opportunity for collaboration, and both communities could benefit greatly from each other. Adding Fintech as a new sub-discipline of digital forensics will foster more collaboration between the digital forensics community and the finance industry.

Ethical and Professional Responsibility in Testimony

Working in the legal system imposes a huge responsibility on you to perform your work with diligence, competence, and good judgment. Computer crimes do not have eyewitnesses, so juries rely on forensics experts to help them understand the meaning of the e-evidence. Jurors are not required to hold any professional qualifications, and there are no technical jury qualification guidelines for cases involving complex computer data. Working as an expert witness can be as challenging as the investigation and perhaps more demanding. You may need to critically review and then validate or refute the testimony of other investigators- or be the subject of another expert’s critique of your methods and opinions. Witnesses need to be prepared to be able to withstand scrutiny from judges, jurors, and attorneys who may know very little

about e-evidence (Computer Forensics US-CERT.). To provide testimony as an expert witness. Given what is at stake, witnesses have ethical responsibilities that cannot be compromised. In addition to understanding the technologies that may be at issue in a given case, to be an effective expert witness you must understand the legal system, specific courtroom communication skills, skills for enduring cross-examination, and how to prepare for legal testimony (Chaturvedi et al, 2019).

Applied research

There is an opportunity for the development of tools and methods to conduct Fintech forensic investigations and evidence acquisition. These tools have many of the same attributes as other digital forensics tools, but with a few subtle differences. For example (Nikkel, 2020):

- focus on understanding the flow and transfer of money
- focus on criminal attribution, helping law enforcement identify individuals
- anomaly detection, finding technical methods to detect technical fraud in progress
- correlating banking infrastructure and transaction logs with criminal activity

How can the digital forensics community contribute to applied research in this area? Attacks involving financial technologies are very technical in nature and include the analysis of hardware, software systems, malware, network protocols, APIs, and cryptography. These are also the primary areas of digital forensics research.Clearly there is opportunity for contribution to the finance industry on the applied research front. Further research is needed to understand how money is flowing from victims to criminals, between criminals, and laundered from criminals back into the legitimate economy - all using cybercriminal methods and infrastructures. The digital forensics aspect of this research is (Nikkel, 2020):

- identify investigative techniques to support law enforcement(going beyond traditional “follow the money” methods)
- provide banks with additional knowledge, tools, and techniques to detect, prevent, and report financial cyber crimes
- define forensic methods and techniques for collecting digital evidence needed for prosecution of criminals
- improve understanding of the darknet and underground economies where criminal financial activity takes place
- provide financial regulators with the knowledge and insight needed to establish appropriate regulation

Some specific areas where the digital forensics community could provide applied research include developing tools and methods for analysis and evidence collection:

- crypto and virtual currencies
- online payment systems
- mobile wallets
- rogue mobile banking apps
- mobile banking malware
- traditional banking malware
- Deep Fake social engineering
- PSD2 and bank APIs
- SWIFT infrastructure and other payment backbones
- corporate payment applications
- peer-to-peer payment systems
- credit card theft
- payment card hardware attacks
- investigative honeypots
- online money laundering
- new sources and locations of digital evidence
- financial fraud event reconstruction
- adding financial activity to technical timelines
- linking investigation and analysis tools to bank proprietary infrastructure
- Fintech forensic readiness
- forensic intelligence related to finance industry relevant crime

Theoretical foundations

Research into Fintech forensics needs to take into consideration existing literature in the area of fraud research. Financial fraud is a well-known problem and has been extensively studied. Research work by the digital forensics' community should seek to extend or compliment this existing body of work from a technological angle, avoiding duplication. The finance industry and traditional fraud research communities have their own taxonomies, frameworks, and nomenclature that can be adopted by the digital forensics' community. Theoretical research into Fintech problems should align or at least not conflict with research conducted in traditional fraud research communities. There are a number of opportunities for conducting Fintech forensic research and several examples are described here.Digital evidence in the context of financial technologies could be studied further. For example (Nikkel, 2020):

- researching the potential differences in digital evidence within the context of Fintech investigations,
- understanding the acquisition of digital evidence in a Fintech incident, especially from dynamically changing evidence sources,
- authenticating the digital evidence acquired, corroborating with other sources of evidence,
- extending, adapting, or validating existing digital forensics research for applicability in a Fintech forensic context.

The forensic analysis and investigative components of Fintech incidents can be studied further. For example:

- how well do existing digital forensic investigation methods apply to the investigation of financial technologies involving the transfer of funds?
- can existing fraud investigation methods be applied or harmonized with existing digital forensic investigation methods?
- can we formalize the concept of “follow the money” in a technical context to support attribution?

From a digital evidence perspective, there are already some advantages built into the financial system that support digital forensic investigation. Regulatory requirements demand extensive data retention, logging, and transaction audit trails. These differ between jurisdictions, but in general provide a level of forensic readiness which can support Fintech forensic investigations. Research collaboration between banks and universities in the area of cyber fraud research could be improved. The Bern University of Applied Sciences held workshops in 2018 and 2019 (called “Bankademia”) with the intention of bringing together researchers from academia and security/fraud practitioners from banks. The results of these discussions highlighted the potential for more collaboration in the fight against financially motivated crime (Nikkel, 2020).

Conclusion

Fintech forensics has many challenges for investigators. These challenges become more and more complex because criminals also learn to hide evidences or have advanced computers knowledge. It was examined distinctive forensic tools used for analysing security flaws in digital forensics and also the detailed review of Fintech forensics. Due to rapid increase in the number of Internet users across the world, the frequency of digital attacks has increased. Therefore, the need to devise effective methodologies and develop efficient tools to detect these attacks timely (Chaturvedi et al, 2019).

Now the main question is this where is this sub-discipline of digital forensics headed? Is there a future for more Fintech forensic research and development? Research in this area is of value to a number of parties:

- banks and Fintech firms: benefit from having new tools and techniques to detect, prevent, and investigate fraud against Fintech systems,
- law enforcement: benefit from new methods and techniques to investigate new Fintech crimes and identify criminals,

- insurance: benefit from understanding Fintech criminal risks for the purpose of defining and managing cyber insurance (claims, etc.)
- regulators: benefit from knowledge of new problems on the horizon which help develop new regulations to protect banks and their clients.

Criminals are clever and creative. Where there is money to be stolen, there will be smart people figuring out how to steal it. Over the past decade technical exploitation has become more difficult as hardware and software vendors have increased their focus on the security of devices, operating systems and applications. During this time social engineering has dramatically increased, exploiting human weaknesses (trust, fear, etc.). In the coming years the human target will be exploited using new technical tools such as Deep-Fakes. These are based on artificial intelligence and will become increasingly difficult for people to detect. However, this technological advancement also brings with it more evidential artifacts which can be analyzed to understand attacks. Another area which will become interesting from a Fintech forensic perspective is the plethora of payment systems on the market. At the moment the number of payment systems continues to grow, and the risk of fraud grows with it. Most of these new payment systems are designed to be mobile, peer-to-peer, and highly scalable. Until this payment system landscape begins to consolidate and mature, there will be a need for Fintech forensic investigation. Open and distributed crypto currencies will likely become more closely interfaced with the traditional financial system over time.

As banks and Fintech startups begin to integrate crypto currencies into their online platforms, there will be an increase of fraud involving crypto currencies. This will include both theft and abuse of crypto currencies. Another interesting aspect of crypto currencies is the possibility of eliminating human mules from the money laundering process. Today laundering stolen funds is inefficient and time consuming. Once crypto currencies become more tightly integrated into online financial platforms, the human money mule can be removed from the loop to potentially allow automated money laundering.

Other areas of technical fraud will include the use and abuse of social media platforms to commit social engineering for fraud. Fintech startups using bank APIs for apps and platforms will become a target of criminals to commit fraud. We may see well established areas such as AML and Financial Crimes leveraging the tools and research produced in the Fintech forensic space. Terrorist financing, sanctions violations, and other traditionally separate areas of finance industry compliance may also see a benefit in using Fintech forensic research and tools. The use and abuse of financial technologies for criminal purposes will continue to grow in the future. The current digital forensics community is well positioned to play a leading role in the research and development of Fintech forensics as a sub-discipline of digital forensics. Technical analysis of financial technologies fits logically within the current domain of digital forensics. Practitioners and researchers in the digital forensics' community have a great opportunity to support the finance industry in the analysis of crime involving financial technology. Also, the existing community of practitioners on the finance industry side can benefit from more interaction with the digital forensics' community. The intent of this paper is to reveal the common ground between the finance industry practitioners and the digital forensics community, and bring these two groups closer together (Nikkel, 2020).

References

Beals, M., DeLiema, M., Deevy, M. (2015). Framework for a Taxonomy of Fraud. Stanford Center on Longevity,

Chaturvedi. A, Awasthi. A & Shanker. S. (2019). Cyber Forensic – A Literature Review. Trinity Journal of Management, IT & Media. Volume-10, Issue-1 (Jan-Dec),

DFRWS. (2001). Collective work of all attendees. In: From the proceedings of The Digital Forensic

Research Conference (DFRWS). USA, Utica, NY,

Faccia. A, Moşteanu. NR, Cavaliere. LPL & Mataruna-Dos-Santos, LG. (2019). Electronic Money Laundering, The Dark Side of Fintech An Overview of the Most Recent Cases. Association for Computing Machinery ICIME 2020, September 16–18, 2020, Amsterdam, Netherlands,

Garber L. (2001). Encase: A case study in computer-forensic technology. IEEE Computer Magazine January,

Haffke, L., Fromberger, M., & Zimmermann, P. (2019). Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them. Journal of Banking Regulation, 1-14,

Nikkel. B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. Forensic Science International: Digital Investigation,

Patrick Schueffel. J. Innov. Manag. (2016). Taming the Beast: a scientific definition of Fintech, JIM 4,

Pedneault. P, Rudewicz. F, Sheetz. M & Silverstone. H. (2012). Forensic Accounting and Fraud Investigation. John Wiley & Sons. 3rd Edition,

Shevchenko. (2016). "Two Bytes to $951M", BAE Systems Threat Research Blog,

Weber, J., & Kruisbergen, E. W. (2019). Criminal markets: the dark web, money laundering and counterstrategies-An overview of the 10th Research Conference on Organized Crime. Trends in Organized Crime, 22(3), 346-356,

International Journal of Financial Technology
(FinTech)
سال (۲) / شماره (۵) / تابستان ۲۰۲۵