Fintech Forensics: Criminal Investigation and Digital Evidence in Financial Technologies

by Bruce Nikkel

bruce.nikkel@bfh.ch

April 10, 2020

Abstract

This paper describes an emerging sub-discipline of digital forensics covering financial technologies, or Fintech. The digital transformation of society is introducing new Fintech for payments, funds transfer, and other financial transactions. Criminals are using and abusing 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.

Keywords: Fintech, Cybercrime, Cyberfraud, Underground Economy, Phishing, Finance, Crypto Currency, Money Laundering

Contents

1 Introduction

This paper describes an emerging sub-discipline 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 underground. The mechanisms used for processing these financial transactions are highly technical involving hardware, software, APIs, cryptography and network protocols. The digital forensics community is already equipped with the technical skills and knowledge to analyze and investigate the underlying technologies of Fintech systems. This can be leveraged to provide end-to-end forensic analysis and post-mortem reconstruction of incidents involving technical financial activity. Theoretical and applied research will result in the development of new frameworks, methodologies, tools and techniques for enhancing investigations involving financial technology and technical ”follow the money” processes.

This paper argues for the recognition of *Fintech Forensics* as a sub-discipline of digital forensics. A definition of *Fintech Forensics* is developed here within the context of accepted definitions of digital forensics. A variety of incident scenarios involving both the use and abuse of financial technologies are discussed to help illustrate the scope of *Fintech Forensics.* The scenarios are described in the context of digital forensic analysis, investigation, and securing digital evidence. This includes financial technologies and services offered by the traditional finance industry, Fintech startups, and open source decentralized technologies. Incidents may involve the use (and abuse) of traditional financial infrastructure, new online or mobile payment systems, independent distributed crypto currency systems, or financial activity in the criminal underground.

The practitioner aspect of Fintech forensics is discussed, including tools and processes used. Much of the practitioner activity described in this paper is not new, and has developed out of necessity within the finance industry. These existing practitioner communities would benefit greatly from more direct involvement with the digital forensics community. 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.

2 Defining Fintech forensics

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.

2.1 Definition of Fintech

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”[1]. Here the author 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. Traditional banks have a history of innovation and introducing new financial technologies. For example ATMs (Automated Teller Machines) were a revolutionary idea in the 1960s and 1970s. In the 1980s banks developed dial-up systems for personal computers with modems to access bank terminal applications. With the growth of the Internet in the 1990s, banks developed online banking portals for clients. The credit card companies introduced new technologies to facilitate online purchasing, and entirely new payment systems such as PayPal were introduced. More recently payment systems were introduced to leverage the pervasiveness of smart mobile devices. Some are developed by the mobile device manufacturers such as Apple Pay[2] or Samsung Pay[3], others are developed by online services companies such as Google Pay[4] or Amazon Pay[5]. Regional initiatives like TWINT[6] in Switzerland involve the collaboration of the local financial community to develop shared products. The future of payment systems and online currencies is still developing, for example, Facebook’s Libra[7] was recently announced as a global currency alternative.

Another growing group of financial technologies are community driven, free and open source. For example, GNU Taler[8] offers an online payment system that protects the privacy of individuals sending payments, but makes the recipient of a transaction transparent for regulatory bodies. 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.

2.2 Developing a definition of Fintech forensics

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

"**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."[10]

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.

3 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[11].

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:

- 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[12].

3.1 Phishing methods for committing financial fraud

Classic phishing[1] 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 monitized.

Smishing, or SMS phishing, involves sending victims a text message impersonating a finanical 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.

3.2 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.

[1] sometimes called "Dinosaur Phish" by the finance industry

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 ”Jackpotting”, 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[2].

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.

3.3 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.

3.4 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.

[2] Carbanak is a good example of such attacks.

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.

3.5 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.

Ransomeware 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.

3.6 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 research[3] 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 finacial 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.

[3] One of the best sources of information is a company's Jobs/Careers page, where job postings often describe internal processes and infrastructure in great detail.

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.

3.7 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.

3.8 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[13]. 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[9] 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.

3.9 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[4].

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 subdiscipline of Fintech forensics is the ability to analyze crypto currencies used by criminals.

3.10 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

[4] In the finance industry having information about the identities of people is referred to as "KYC", or "Know Your Customer"

services from other criminals (”Crime-as-a-Service” model). Some examples include:

- operating illegal online web sites and forums (bullet-proof hosting)
- providing reliable spam campaigns to distribute emails with malicious web links or attachments
- renting of multipurpose botnets (large numbers of infected devices which are centrally controlled by a criminal actor)
- selling or renting phishing kits to steal credentials for identity theft
- selling or renting online banking trojans for unauthorized access to bank accounts to make fraudulent payments
- 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:

- physical contraband such as drugs or weapons
- illegal material (pictures/videos) involving child sexual exploitation or extreme violence
- 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.

4 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.

4.1 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 10-15 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.

4.2 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:

- 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 cyber-criminal methods and infrastructures. The digital forensics aspect of this research is to:

- 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
- DeepFake 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

There are significant applied research possibilities for the digital forensics community to contribute to the finance industry in the area of Fintech forensics.

4.3 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:

- 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.

5 The future of Fintech forensics

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 DeepFakes. 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.

References

[1] Taming the Beast: A Scientific Definition of Fintech, Patrick Schueffel, Journal of Innovation Management JIM 4(2016), ISSN 2183-0606

[2] Apple Inc., ”Apple Pay”, https://www.apple.com/apple-pay/, accessed 2020-01-10

[3] Samsung Electronics, ”Samsung Pay”, https://www.samsung.com/us/samsung-pay/, accessed 2020-01-10

[4] Google LLC, ”Google Pay”, https://pay.google.com/, accessed 2020-01-10

[5] Amazon.com Inc., ”Amazon Pay”, https://pay.amazon.com/, accessed 2020-01-10

[6] TWINT AG, ”TWINT”, https://www.twint.ch, accessed 2020-01-10

[7] Libre Association, Facebook Inc., ”Libra”, https://libra.org, https://github.com/libra/libra, accessed 2020-01-10

[8] Taler Systems SA, ”GNU Taler”, https://www.taler.net, accessed 2020-01-10

[9] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366, 2015-11-25

[10] Collective work of all DFRWS attendees, From the proceedings of The Digital Forensic Research Conference (DFRWS), 2001 USA, Utica, NY

[11] Europol, "Internet Organised Crime Threat Assessment (IOCTA)", https://www.europol.europa.eu/iocta-report, accessed 2020-01-10

[12] M. Beals, M. DeLiema, M. Deevy, "FRAMEWORK FOR A TAXONOMY OF FRAUD", Stanford Center on Longevity, July 2015

[13] S. Shevchenko, "Two bytes to $951M", BAE Systems Threat Research Blog, 2016-04-25