IDS 300W
Research Paper
Chris Evans
01206431

Preventing Online Bank Fraud

PART 1 - Steps 1-2

Thesis: Online bank fraud is the use of computers to steal the financial resources and/or authorization of a person or organization. Stopping online bank fraud requires the expertise of many different disciplines and their collective knowledge to secure user identities, accounts, and moneys.

Cybercrime is broadly defined as criminal activities carried out by means of computers or the internet. More specifically Cybercrime can include bank fraud, identity theft, bullying or stalking, hacking, media and software piracy, corporate espionage, extortion, or property theft. This problem is complex, meaning it requires insights from more than one discipline, as many disciplines like sociology, political science, economics, and computer science have written about the effects of Cybercrime on victims, judicial systems, and the development of new computer technologies. The scope of this topic I would like to focus on is online bank fraud in particular, the ways it can be prevented and minimized by potential victims and other stakeholders seeking to solve the issue. In the year 2020 alone, the Federal Trade Commission reported that Americans lost almost $3 billion USD to financial fraud with the incidents only increasing yearly (Brainy.) Worldwide credit card fraud has increased yearly for a decade and in 2016 victims lost out on $24 billion USD (VICE.) Online bank fraud is a problem that can't be left up to users to self-defend or law enforcement to prosecute when they are able to make an arrest. A new interdisciplinary prevention approach is needed to tackle an inherently interdisciplinary crime.

A recent documentary produced by VICE news for YouTube gives us a brief overview of the world of online bank fraud, some of the victims, perpetrators, and methods that are used to commit and defend against online bank fraud. Often a criminal will purchase banking information online from a type of dark web website. The dark web is series of internet websites only accessible by using a Tor Internet browser. This Tor browser allows users a degree of anonymity from Internet service providers and from law enforcement and is the method of choice for people or groups committing crimes online. The dark web is often home to various illegal and criminal related content and activities. Dark websites have been known to sell illegal drugs, weapons, or traffic people as well as offering criminal services. One of the most lucrative criminal acts on the dark web is the sale of large databases of credit card information like account card numbers, expiration dates, and CVV codes as well as other personally identifiable information like names, birth dates, social security numbers and addresses. With this information criminals are able to copy a victims credit card, and make unauthorized purchases online. The criminals often are operating in networks of card information aggregators, card cloners, runners who make the illegal purchases, and often but not always fences who purchase the illegal gotten goods (VICE.)

The interdisciplinary approach to studying the Cybercrime of online bank fraud seems to be a perfect match. The disciplines of political science, computer science, and sociology are just a few of the disciplines that have been consulted by society to address the growing number of online bank frauds and the increasing number of victims. These disciplines have given us some assistance to limit these crimes, such as law enforcement that has worked with computer science and digital forensic analysts to discover new ways to gather evidence and prosecute these criminals. Political science has given us laws and frameworks for understanding what existing laws are broken and what new laws need to be created. And Sociology and computer science have helped us understand who is committing these acts, who is victimized, and what the effects on society have been. However, every existing

discipline has tried to give us their remedy, but they have all been unable to contain or slow the number of online bank frauds that increase every year (Brainy.) These previous disciplines lack the interdisciplinary approach which can incorporate all their previous established insights into making social systems that limit the effects on victims and limit the number of people turning to crime, while also increasing law enforcement's ability to prevent and prosecute and increasing the security of everyone online.

PART 2 - Steps 3-6

Discipline/Sub Discipline	**Insight of Author**
Sociology	Online bank fraud is driven by easy access to the technology that makes the crime possible and limited prosecution of those crimes. Perpetrators feel the crimes are victimless, or the victims are wealthy banks (Ritzer.)
Computer Science/Cybersecurity	Interconnected computer systems like the internet are built upon systems where security was an afterthought, our challenge as Cybersecurity disciplinarians is building secure infrastructure on top of that unsecured base (Newhouse)
Computer Science/Cybersecurity	Online bank fraud leaves trails of digital evidence

	that can be used to assemble reports for law enforcement and eventual prosecution (Vaishnavi Pg. 631-641)
Political Science/Law Enforcement	Online websites exist that assist in educating criminals in how to steal banking information and allow the free sharing of stolen data, crime techniques, and how to evade law enforcement. (DOJ)
Political Science/Law Enforcement	Online bank fraud presents challenges to law enforcement as the crimes often span multiple countries and jurisdictions. Record keeping and digital forensic analysis abilities of various civil authorities may vary significantly. (FTC)

When it comes to online bank fraud two immediate disciplines come to mind as we seek answers in reducing the quantity of victims and impact to their lives. First is law enforcement. A sub-discipline of Political Science. Law enforcement as a branch of government attempts to discover, deter, punish, and rehabilitate people or organizations who violate the civil codes of whatever jurisdiction they represent (New Law.) The law enforcement. perspective on online bank fraud is that they can educate the public on how to prevent themselves from being a victim, and to recognize the signs of potential credit card information theft or skimming. Additionally law enforcement's perspective is that criminals often operate across jurisdictions, and in areas where police presence is weak or non-existent, like rogue nations or online on dark web forums (DOJ.) There is a desire from many in law

enforcement to gain additional technological abilities and legal privileges to seek out where criminals operate online and to stop their activities (FTC.)

The next discipline that comes to mind is that of Cybersecurity, the discipline of ensuring that networked computer systems are dependable, that their data is private, and that their data has not been altered. Cybersecurity experts would have us understand that all the technologies we have today are computers built upon insecure standards and systems. That our great task is to create secure systems on top of inherently insecure systems. When many networking and computer protocols were being created or built there were expectations of trusts between users and very little concern for security or crime. Attempts to secure these computer systems and data are difficult and require expert knowledge (Newhouse.) Another point Cybersecurity experts explain is that all online activity and online bank fraud leaves trails of digital evidence that can be used to assemble reports for law enforcement and eventual prosecution (Vaishnavi Pg. 631-641.) This disciplinary insight is indeed correct and useful for society in our attempt to limit online credit card fraud. All activities that happen on a computer or a computer operating online are logged somewhere. When a user connects to a dark-web website, or attempts to use stolen credit card information online, a log is created as the computers are connecting and communicating. These logs can contain valuable information about the location or source of criminal activity. No actions online are ever one hundred percent anonymous, because the underlying structure of networked computer communications was never designed with anonymous use in mind.

The next discipline that might not come immediately to mind is Sociology. Sociology is the study of society and human interactions, behaviors, or structures. Sociology tells us that online bank fraud is driven by easy access to the technology that makes the crime possible and limited prosecution of those crimes. Perpetrators feel the crimes are victimless, or the victims are wealthy banks (Ritzer.) Sociologist are concerned with why people act the way they do and what impact society or social groups have on our behavior. The insights sociologist contribute to online bank fraud is that it is an

easy and lucrative crime. Many dark websites are available to assist would be criminals in educating them on the methods and techniques for committing online credit card bank fraud. We see additionally that criminals often feel that they are not victimizing another person after stealing their banking information as credit cards often carry fraud protection which reimburses the victim should their card be stolen. This explanation helps criminals remove feelings of guilt from their actions (VICE.) Many criminals also feel that their real victims are wealthy banks, and that these banks have stolen millions of dollars from regular people for years, so it is only fair turn around to steal some of the bank's money as well (Ritzer.)

PART 3 – Steps 7-8

The disciplines presented previously, sociology, Cybersecurity, and law enforcement have each had a hand in attempting to stop online bank fraud and while some progress has been made, online bank fraud with credit cards has increased every year for the last decade until 2016 (VICE.) These insights and perspectives are often at odds with each other. Law enforcement insights are often of the nature that increased government powers and technologies can grant them the ability to shut down credit card database selling websites on the dark web, and to more thoroughly track users online activity. This is met with dissent from many who feel wary of giving the government more powers and legal abilities than they already have, especially in the light of recent abuses of power by law enforcement. agencies. And additionally, the encroachment on users and citizens privacy of their online activities, which many view as privileged and believe should be free from eavesdropping by any organization. Human rights organizations are also wary of the use of increased surveillance technology by law enforcement. and government. A particularly gruesome example of their worries made manifest is the murder of civil rights activist Jamal Khashoggi by the Kingdom of Saudi Arabia in Istanbul, Turkey in 2018. Mr. Khashoggi had his cellphone targeted by Pegasus spyware, which was sold to the

government of Saudi Arabia for the purposes of catching criminals and terrorists but was re-oriented to attack civil dissidents (Bergman.)

Cybersecurity experts insights and recommendations are often difficult to implement as they require user education on technical and deeply niche subjects or they run the risk of becoming seen as arbitrary rules or guidelines. Indeed, often Cybersecurity experts have difficulty securing their devices and networks and the changing landscape of smartphone technology presents a new challenge (DeMuro.) User education is one of the most difficult methods to increase security in computer networks, and as we have seen convenience take precedence over security, we can assume that this will be a tall order in limiting online bank fraud.

Sociology offers other insights that are also in conflict. Most sociological work about the nature of online bank fraud has a bias that criminals are lazy and motivated by easy rewards by attacking soft targets. However, this doesn't take into account how many hours criminals spend learning the techniques for online bank fraud, and the techniques for more secure and private online activity to evade law enforcement. Many times, criminals are able to take advantage of easy dark web websites, however an intelligent criminal or criminal organization had to establish those websites and systems for credit card information theft beforehand. Sociologists often are in conflict with law enforcement as well, as law enforcement seeks to punish criminal behavior and sociologists seek to study, understand and hopefully prevent criminal behavior.

With all this considered what common ground are we able to find. Well for one all the disciplines agree that study of online bank fraud is useful and necessary to gain a deeper understanding of it. Whether is sociological study, or law enforcement surveillance of criminals, or Cybersecurity experts setting honey pots and doing penetration testing on banking infrastructure. This could be all expressed in another way, information empowers action. The more information we can gather about

online bank fraud as disciplinarians, inter-disciplinarians, and as people worried about our safety and privacy of online banking, then the more secure we can be. Doing more work to gain information and data on bank fraud should be considered a primary goal by all stakeholders.

Another common ground is the necessity of that information to be freely passed between invested parties. Jurisdictional disputes can often hamper investigations into online bank fraud and limit police from victim's jurisdictions from reaching criminals in another jurisdiction. The free flow of information would assist law enforcement in being able more effective at stopping this online crime. Additionally, information can dissuade potential online bank fraud criminals from committing their crimes by showing them the consequences for their crimes, and how seriously law enforcement. is working to catch and prosecute them.

PART 4 - Steps 9-10

With our insights collected we can attempt to create a new understanding and integrate them as follows: To help limit and prevent online credit card bank fraud, we should allow more research to be conducted into how the criminals operate and to share this information with as many stakeholders as possible to educate them and create better user habits around online bank information. The expertise of many different disciplines will help create a larger picture on how we can help protect people from these online crimes.

Online bank fraud and the theft of credit cards information is a multi-billion-dollar criminal industry. If we can continue to integrate the understanding of the many expert disciplines and their insights, we can create better methods and techniques for securing peoples identities and finances. This will have a positive effect on society, and on economics, and less crimes are committed, and less people have their lives affected.

REFERENCES

Alhabeeb, MJ, "Expressing America: A critique of the global credit card society - Ritzer,G" (1997). International Journal of Comparative Sociology. 2. Retrieved from https://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1001&context=resec_faculty_pubs

Newhouse, Bill. *Securing Property Management* Systems. Mar 30, 2022. National Institute of Standards and Technology. Accessed Jun 29, 2022. https://www.nist.gov/publications/securing-property-management-systems

New Law Journal - Volume 123, Part 1 - Page 358, 1974

R. Bergman and M. Mazzetti, "The battle for the worlds most powerful cyberweapon," *New York Times*, Jan. 31, 2022, **https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html** , [accessed Apr. 6, 2022]

J. DeMuro, "8 reasons why smartphones are privacy nightmare," *Tech Radar,* Feb. 8, 2021, **https://www.techradar.com/news/8-reasons-why-smartphones-are-privacy-nightmare** , [accessed Apr. 6, 2022]

Tech Support Scams. Mar 30, 2022. Federal Trade Commission. Accessed Jun 29, 2022. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/tech-support-scams

U.S. Attorneys Office Eastern District of Virginia. April 12, 2022. United States Department of Justice. Accessed Jun 29, 2022. https://www.justice.gov/usao-edva/pr/us-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator

Whitney, Lance. Dark *Web Credit card fraud less pervasive but still an ongoing problem.* Aug 1, 2022. Tech Republic. Accessed Aug 1, 2022. https://www.techrepublic.com/article/dark-web-credit-card-fraud-less-pervasive-but-still-an-ongoing-problem/

Vaishnavi Nath Dornadula, S Geetha,
Credit Card Fraud Detection using Machine Learning Algorithms, Procedia Computer Science, Volume 165, 2019, Pages 631-641, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.01.057.

(https://www.sciencedirect.com/science/article/pii/S187705092030065X)

VICE. (2018, June, 8) *Credit Card Scammers on the Dark Web.* [Video]. YouTube. https://youtu.be/jT-jmq8KBw0