How Shifting Liability Explains Rising Cybercrime Costs

Tyler Moore

School of Cyber Studies, College of Engineering & Computer Science,
The University of Tulsa, OK, USA tyler-moore@utulsa.edu

Abstract. The extent and cost of cybercrime has grown substantially in recent years. One underappreciated reason why is that for many such crimes, intermediaries such as banks have successfully avoided liability for fraud. Using a case study and data from the FBI's Internet Crime Complaint Center, this paper demonstrates how the financial losses arising from cybercrimes where liability is assigned to financial institutions are dwarfed by crimes where it is not. The paper then discusses circumstances under which liability for these cybercrimes should be assigned to parties other than individual victims.

1 Introduction

In his seminal paper "Why cryptosystems fail", Anderson observed that US and UK bank regulation differed in terms of who was ultimately held responsible for paying for ATM card fraud [1]. In the US, the rules were clear: banks are liable for ATM fraud. In the UK, banks could frequently require customers to shoulder the costs of fraud. In technological respects, UK and US banks were quite similar. This policy difference led to vastly different outcomes, with UK banks experiencing higher overall fraud losses per capita. This early insight about the importance of incentives contributed to the emergence of the security economics as a subdiscipline of cybersecurity [2].

In the decades since, many new forms of cybercrime have proliferated. While the composite magnitude of the costs imposed by these cybercrimes have proven difficult to measure [3, 4], it is clear that some categories cause much greater financial losses than others. This paper will argue that whenever intermediaries, such as banks, technology platforms and payment service providers, are held liable for cybercrime costs, they do a pretty good job managing the risk and minimizing overall fraud losses. Cybercrimes in this category includes phishing attacks and payment card fraud. However, when intermediaries can avoid liability for losses and instead place the burden of cybercrime on individuals and smaller enterprises, cybercrime costs have exploded. In fact, I argue that this is a natural reflection of the incentives at play for attackers and defenders alike. Cybercriminals are naturally drawn to attacks that avoid the ire of banks and technology platforms, as these attacks are more profitable and face less resistance. Defenders meanwhile do not place as much emphasis on countering such threats for the simple reason that they do not bear the cost of the attacks.

2 Case Study: PayPal Fraud

The following case study experienced by the author illustrates the problem. On April 26, 2024, I received a payment request through PayPal from "Loretta Simmons" for $789.99. Such a request is not unusual. My PayPal account is shared with my spouse. She collects vintage goods and occasionally purchases items from people she interacts with online. When requests like these arrive, we communicate through an out-of-band channel to verify whether the payment request is expected. In this case, she texted me, "Did you see that PayPal money request?", to which I replied with the details of the transaction. I misinterpreted this communication as confirmation that the transaction was valid, so I completed payment, using the "friends and family" option.

The next evening over dinner when I asked about what she had bought, she told me that she did not buy anything through PayPal. That is when I realized we had miscommunicated earlier and I had been scammed. What followed illustrates how when liability for fraud falls on consumers, it is easily ignored by intermediaries.

I called PayPal. I initiated a dispute through the automated system. A case was opened at 8:46PM. At 9:04PM, I received another email notifying me that my case had been closed, and they "determined there was no unauthorized use". They suggested I contact the seller (i.e., the scammer) to try to resolve my dispute. I immediately called PayPal again, only to find that the call center closed for the day at 9PM. I got through to a human operator on April 29, who again advised me to contact the seller to resolve the dispute. When I explained that the seller was in on the fraud, I was told to contact my bank to try to stop the payment. I immediately contacted the bank and disputed the transaction; unfortunately, the payment cleared at 4AM on April 29 and the bank refused reimbursement, stating that I should seek restitution from PayPal. Ultimately, neither PayPal nor the bank reimbursed me for the fraud.

What lessons can be learned from this experience? One is that PayPal's own processes are not optimized to assist customers who experience fraud initiated on its platform. The messaging and investigation focused on mediating disputes between legitimate buyers and sellers, as well as account takeovers. PayPal's investigation confirmed that I initiated the payment (which I never disputed doing), and then used that information to determine that they were not liable.

When payments are made to bank accounts controlled by scammers, acting quickly is essential to reversing fraudulent payments. Yet PayPal's initial messaging, both when I opened the dispute investigation and when it was quickly closed, made no recommendation that I contact my bank to dispute the transaction. Because the payment did not post until more than 24 hours after those communications, a faster response would likely have foiled the fraud. PayPal is not incentivized to assist customers in this manner, as the liability for fraud had been determined to lie with the customer.

Additionally, neither of the two operators I spoke with encouraged me to file a police report. When I asked if I should do so, I was told that is up to me and that was something they could not assist with.

3 Liability and Self-Reported Cybercrime Losses

	2023		2022		2021	
	#	$ Loss	#	$ Loss	#	$ Loss
Cybercrime Categories Where Intermediaries are Usually Liable						
Credit Card/Check Fraud	13718	173.6M	22985	264.1M	16750	173.0M
Identity Theft	19778	126.2M	27922	189.2M	51629	278.3M
Non-Payment/Non-Delivery	50523	309.6M	51679	281.8M	82478	337.5M
Phishing/Spoofing	298878	18.7M	321136	160.0M	342494	126.4M
Total (Liable)	382897	628.2M	423722	895.1M	493351	915.1M
Cybercrime Categories Where Intermediaries are Usually Not Liable						
Advanced Fee	8045	134.5M	11264	104.3M	11034	98.7M
BEC	21489	2946.8M	21832	2742.4M	19954	2396.0M
Confidence Fraud/Romance	17823	652.5M	19021	735.9M	24299	956.0M
Employment	15443	70.2M	14946	52.2M	15253	47.2M
Extortion	48223	74.8M	39416	54.3M	39360	60.6M
Investment	39570	4570.3M	30529	3311.7M	20561	1455.9M
Lottery/Sweepstakes/Inheritance	4168	94.5M	5650	83.6M	5991	71.3M
Overpayment	4144	38.3M	6183	33.4M	6108	
Ransomware	2825	59.6M	2385	34.4M	3729	49.2M
Real Estate	9521	145.2M	11727	396.9M	11578	350.3M
Tech Support	37560	924.5M	32538	806.6M	23903	347.7M
Total (Not Liable)	299996	11489.4M	290828	9912.8M	253468	6666.3M

Table 1. Cybercrime losses from 2021–2023 according to the FBI IC3.

The US FBI operates the Internet Crime Complaint Center (IC3), which collects reports of cybercrimes experienced by individuals and organizations. Each year the IC3 releases a report detailing cybercrime incidents and financial losses, split by various categories [11–13].

Table 1 reports the figures for cybercrime categories that generate financial losses. It does not include categories of harms where no explicit financial loss is experienced, such as harassment, stalking, and crimes against children. I have also excluded infrastructure crimes such as botnets and malware.

The cybercrimes are split into two categories. At the top are crimes where fraud liability rests with intermediaries such as financial institutions. At the bottom are crimes where responsibility typically falls on the individuals involved.

In terms of the number of incidents reported, cybercrimes where individuals are not usually liable outnumber those where individuals are responsible, with 400–500K reports annually compared to 250–300K reports. These totals are heavily skewed by phishing, which accounts for the majority of all reports where banks are liable.

Despite a higher incidence of crimes, the amount of money lost to scams is much higher in cases where individuals are liable. In 2023, for example, losses due to these frauds totaled $11.5 billion, compared to $628 million for cases where banks and other intermediaries are liable. A similar trend holds for 2022 and 2021 as well – frauds where intermediaries avoid liability report an order of magnitude more financial losses than crimes where they foot the bill.

What drives these differences? Incentives provide the simplest explanation. When banks and other financial intermediaries are responsible for managing cybercrime risks, they do a respectable job reining in losses. For example, I have seen in the past two decades significant investment in countermeasures to combat phishing [8, 9]. Consequently, while the number of phishing attacks remains high, reported losses are quite small (roughly $100 million annually according to IC3 data).

For crimes whose losses are borne directly by the victims, losses are much higher. For example, business-email compromise (BEC) reports annual losses of $2-3 billion. Here, firms are duped into paying fake invoices worth hundreds of thousands of dollars to scammers. While banks do cooperate with investigations and try to block these payments from clearing, they often fail. And when they fail, it's the bank's customer who pays.

The "least-cost avoider" principle from tort law which holds that liability should be assigned to the party that can avoid harm for the lowest cost [5]. It is clear that for phishing, identity theft and credit-card fraud, payment intermediaries can avoid the costs of these crimes more efficiently than individuals and organizations could. This is because the intermediaries have greater technical expertise and visibility into the crimes targeting their customers.

What about the other crime categories listed in Table 1 where intermediaries are not currently liable? In most cases, they are in a much better position to counter cybercrime risks than victim individuals and organizations. Take BEC. Each year, tens of thousands of organizations are targeted. While these organizations can and should invest in efforts to tighten protocols around payments to vendors, victims typically have never experienced these attacks until they are targeted. By contrast, financial institutions have been dealing with BEC attacks targeting their customers for years. They have access to transaction data, which can reveal anomalous patterns. They can purchase software from third-party vendors to identify suspected BEC scams. Put simply, banks are the least-cost avoider for BEC.

Also key to assigning liability responsibility is the extent to which an intermediary can be aware of the attack taking place and how their platform is utilized in the attack. These concepts are often interrelated. For example, in many advanced fee frauds, the cash-out mechanism is a money-services business like Western Union or Moneygram. Here, the operator typically does not know what the payment is being used for. In this case, it is not clear that the payment processor is in a strong position to detect and block the fraud.

The PayPal case study from Section 2 nicely illustrates how payment platforms may be utilized and aware of crimes they help facilitate. In contrast to

advanced fee frauds, lottery scams, BEC, and others, the platform itself was utilized to initiate the scam. I received a valid payment request initiated through PayPal by an illicit user. PayPal permitted "Loretta Simmons" to sign up for an account, associate a bank account, and submit payment requests (of which I was likely only one of many recipients). Hence, PayPal's platform was integral to several stages of the scam's operation. Moreover, this integration also ensures that PayPal has good awareness to the scam, and by extension, is in a strong position to mitigate the harms. The fact that it failed to detect or counter the attack (after being notified) can best be explained by the fact that they were not held financially responsible.

Finally, it is worth noting that there can be cases where no payment intermediary exists. Most ransomware attacks are monetized through Bitcoin payments. Victims pay directly to addresses established by cybercriminals. A similar approach is utilized in so-called "pig butchering" schemes. While these scams may appear to leverage a fully decentralized payment infrastructure, in practice they often hold accounts at one of the centralized cryptocurrency exchanges [6, 10]. Hence, even in these cases intermediaries may be available where pressure could be applied if desired.

4 Discussion and Concluding Remarks

Experience has demonstrated that the harms resulting from cybercrime can be mitigated to a socially-acceptable level. The key is to get the incentives right. I have shown that when liability for cybercrimes is placed on the party in the best position to defend against attacks, harms are lower. Unfortunately, cybercriminals often behave rationally. Many have shifted their efforts away from crimes that banks and other platforms are focused on reducing. Instead, criminals have turned their attention to scams where such well-resourced intermediaries are not liable and therefore are not devoting as much effort to stop.

What are the policy implications? If reducing overall societal harm is the goal, then responsibility for more cybercrimes need to shift away from individual victims to the intermediaries in the best position to take precautions. Such an approach may not always be popular, particularly when intermediaries could argue that they are not the ones responsible for insecure or otherwise poor decisions taken by their customers. Yet the principle of indirect intermediary liability does not require liability to be placed on the party most responsible [7]. It holds that the party in the best position to counter the risk should be the one assigned responsibility for doing so.

One way to honor Ross Anderson's legacy is to continue to fight for the many individuals who fall victim to cybercrimes and are held financially responsible even when responsibility should lie elsewhere. This paper has shown one strategy for doing so.

References

1. Anderson, R.: Why Cryptosystems Fail. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. pp. 215 – 227. CCS '93, Association for Computing Machinery, New York, NY, USA (1993). https://doi.org/10.1145/168588.168615, https://doi.org/10.1145/168588.168615
2. Anderson, R.: Why information security is hard - an economic perspective. In: Seventeenth Annual Computer Security Applications Conference. pp. 358–365 (2001). https://doi.org/10.1109/ACSAC.2001.991552
3. Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M.v., Levi, M., Moore, T., Savage, S.: Measuring the Cost of Cybercrime. In: 11th Workshop on the Economics of Information Security (WEIS) (2012), https://tylermoore.utulsa.edu/weis12.pdf
4. Anderson, R., Barton, C., Böhme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., Savage, S., Vasek, M.: Measuring the Changing Cost of Cybercrime. In: 18th Workshop on the Economics of Information Security (WEIS) (2019), https://tylermoore.utulsa.edu/weis19cost.pdf
5. Calabresi, G., Melamed, A.D.: Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. Harvard Law Review **85**(6), 1089 (Apr 1972). https://doi.org/10.2307/1340059, https://www.jstor.org/stable/1340059?origin=crossref
6. Griffin, J.M., Mei, K.: How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering (Feb 2024). https://doi.org/10.2139/ssrn.4742235, https://papers.ssrn.com/abstract=4742235
7. Moore, T.: The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection **3**(3), 103–117 (Dec 2010). https://doi.org/10.1016/j.ijcip.2010.10.002, https://www.sciencedirect.com/science/article/pii/S1874548210000429
8. Moore, T., Clayton, R.: Examining the impact of website take-down on phishing. In: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. pp. 1–13. eCrime '07, Association for Computing Machinery, New York, NY, USA (Oct 2007). https://doi.org/10.1145/1299015.1299016, https://doi.org/10.1145/1299015.1299016
9. Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis, J., Zand, A., Thomas, K., Doupé, A., Ahn, G.J.: Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale. In: USENIX Security Symposium. pp. 361–377 (2020), https://www.usenix.org/conference/usenixsecurity20/presentation/oest-sunrise
10. Ordekian, M., Papasavva, A., Mariconti, E., Vasek, M.: A sinister fattening: Dissecting the tales of pig butchering and other cryptocurrency scams. In: 2024 Symposium on Electronic Crime Research (eCrime 2024) (2024)
11. US Federal Bureau of Investigation: Internet crime report (2021), https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf
12. US Federal Bureau of Investigation: Internet crime report (2022), https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf
13. US Federal Bureau of Investigation: Internet crime report (2023), https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf