Cyber Threats, Consumer Data, and the Financial System

Before the U.S. House of Representatives
Committee on Financial Services
Subcommittee on Consumer Protection and Financial Institutions

November 3, 2021

Testimony of
Samir Jain, Director of Policy, Center for Democracy and Technology

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to testify about cyber threats and consumer data in the financial system. CDT is a nonpartisan, nonprofit 501(c)(3) charitable organization dedicated to advancing civil rights and civil liberties in the digital world. For over 25 years, CDT has championed policies, laws, and technical designs that empower individuals and communities to use technology for good – while protecting against invasive, discriminatory, and exploitative uses. CDT works to promote privacy, security, and other human rights online by holding governments and companies accountable for the ways they shape our online environment. CDT has offices in Washington, D.C., and Brussels, and has a diverse funding portfolio from foundation grants, corporate donations, and individual donations.[1]

In my statement, I will make some observations about the cyber threat environment, highlight three of the challenges we face in addressing these threats, particularly in the financial services sector, and discuss several potential areas in which we can and should make progress to better protect consumers and their data.

[1] Annual Report: Center for Democracy & Technology, https://cdt.org/wp-content/uploads/2021/06/CDT_Annual_Report_2020_spreads_small.pdf

The Cyber Threat Environment

Despite continued efforts by the U.S. government and greater consciousness in the private sector about the threat of malicious cyber activity, the cyber threat environment has grown more dangerous. At a Department of Justice cyber roundtable that I attended a few weeks ago, Deputy Attorney General Lisa Monaco observed that cyber threat actors have grown "more aggressive; more sophisticated; and more belligerent" since her service as homeland security advisor during the Obama Administration.[2]

From my vantage point, having represented clients in cybersecurity matters after leaving government, and then joining CDT at the beginning of this year, that is clearly true. Cyber threats are becoming more dangerous and disruptive. A decade ago, cyber incidents generally involved temporary denial of service attacks and stealing intellectual property, personal information, or money. While those all persist today, cyber attacks now increasingly involve more disruptive activity, including activity aimed at critical infrastructure such as financial services. The result can be disruption of basic functions such as power or access to fuel or even physical harm, as may have occurred when a ransomware attack on a hospital allegedly resulted in a baby getting substandard medical care and tragically dying.[3] As we grow ever more connected – whether through deployment of the so-called Internet of Things or, in the case of financial services, developments such as the growth of fintech – cyber incidents are likely to continue to become more numerous and cause greater disruptions and harm to individuals.

One clear manifestation of this trend is the proliferation of ransomware attacks. Ransomware has typically involved use of malware to encrypt the data on a victim's systems and demand for a ransom payment in exchange for the victim regaining access to the data. In the last year or two, however, ransomware actors have increasingly taken to not only holding access to data hostage, but also stealing

---

[2] Remarks of Deputy Attorney General Lisa Monaco, Cybersecurity Roundtable on "The Evolving Cyber Threat Landscape," October 20, 2021, *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr.

[3] Kevin Poulson, *et al.*, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," Wall St. J., September 30, 2021, *available at* https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.

private information prior to encrypting it and then threatening to publish that data if the victim does not pay the ransom. Indeed, as many as 70% of ransomware attacks reportedly involved that dual threat as of the end of last year.[4] And financial services are a primary target of ransomware attacks. According to the cybersecurity firm Trend Micro, the banking industry experienced a **1318%** year-over-year increase in ransomware attacks in the first half of 2021.[5]

Some of the Challenges in Addressing the Increased Cyber Threat

The financial services industry overall has responded earlier, with greater investment, and more proactively to cybersecurity challenges than most other sectors. Yet it still remains highly vulnerable to cyber threats. There are myriad reasons why cyber threats are so difficult to address, ranging from difficulties in attributing an attack to a particular actor to being able to then take action against that actor, particularly when they are located overseas. Here, I'd like to focus on three challenges that are particularly pertinent to the financial services industry.

Interdependence with vendors, third parties, and other sectors. Financial institutions are highly interconnected with one another and with third-party service providers and vendors that have access to their systems and/or data. As a result, a financial institution cannot just be focused on its own cybersecurity. Rather, it must take account of cybersecurity in managing its relationships with vendors by undertaking due diligence of their security practices and conducting oversight and monitoring, including potentially requiring security audits and penetration tests.

This interdependence has significant implications from a systemic point of view. For example, because financial networks are connected with one another, a cyber attack can spread rapidly across the financial sector as an attacker moves laterally across these connections. Moreover, to the extent that many financial institutions rely on a common vendor for products or services, a successful attack on that single vendor can have sector-wide consequences.

---

[4] Coveware, "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," Feb. 1, 2021, *available at* https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020.

[5] Trend Micro, "Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats," Sept. 14, 2021, *available at* https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats

We saw a version of that dependency with the SolarWinds cyber incident earlier this year. SolarWinds is a company that develops software to help businesses manage their networks and systems – it's a company that most Americans and policymakers probably had never previously heard of and likely would not have appeared on anyone's list of prominent potential cyber targets. Yet because thousands of businesses, large and small, rely on SolarWinds software, the malware that was introduced as part of a seemingly routine software update propagated across many of those business and resulted in one of the largest and most damaging cyber incidents in our history. As the Superintendent of New York's Department of Financial Services observed in the wake of the incident, "[s]eeing hackers get access to thousands of organizations in one stroke underscores that cyber attacks threaten not just individual companies but also the stability of the financial industry as a whole."[6]

As the SolarWinds example illustrates, the financial sector is not only internally interdependent, but dependent on many other sectors. That is true of information technology, including both hardware and software. But it also true of energy: if a utility suffers a cyberattack and cannot provide power, financial institutions served by that utility may not be able to function. The same could happen if a communications service provider is taken down by a cyber attack. Thus, at some level, reducing cyber risk for the financial system requires reducing risk for the ecosystem as a whole.

Gap between large and small institutions. The largest financial institutions devote tremendous resources to addressing cyber risks. For example, they have significant in-house cyber expertise (often with deep law enforcement or national security experience), can supplement that as needed with outside expertise, can develop or purchase the most sophisticated defensive products and services, and have the reach to engage in operational collaboration with the government.

But regional and community financial institutions do not have those resources or capabilities. Like those in many other sectors, they may often have limited in-house cyber expertise, do not have the reach to work directly with the federal

---

[6] Finextra, "NYDFS: SolarWinds hack is a harbinger of the next big financial crisis," May 4, 2021, *available at* https://www.finextra.com/newsarticle/37979/nydfs-solarwinds-hack-is-a-harbinger-of-the-next-big-financial-crisis.

government, and have limited budgets to devote to cybersecurity. Moreover, they may be particularly dependent on service providers and other third parties for various capabilities. Nor are these entities immune from attack because they are small: in 2020 over a quarter of breaches involved small business victims.[7] Moreover, because of the interconnectedness and interdependence noted above, a successful cyber attack on one small financial institution may well not stay confined to that institution. As a result, any realistic assessment of cyber risks to the financial system cannot simply look to the bigger banks, but must assess the full range of financial institutions.

Increasing reliance on technology. The financial system is increasingly dependent on the Internet, private networks, servers, and other technologies. Today, customers interact with the financial system through technology even for traditional banking services, such as through an ATM or online banking services. The days of writing (non-electronic) checks and visiting physical bank branches are rapidly coming to an end. As a result, the financial sector is increasingly subject to disruption as a result of cyber attacks.

That is all the more true once you look beyond traditional banks to the rise of fintech, open banking and data aggregators, and the increased involvement of large technology platforms such as Google, Facebook, and Apple in the provision of financial services. Financial data is proliferating across the digital ecosystem and with that comes increasing risk to the privacy and security of consumer data and the integrity of the financial system.

Areas for Progress

Both the government and private sector have been seeking to develop strategies for addressing cyber threats for a number of years, and much work remains to be done. I want to highlight three areas where Congress should look to make greater progress.

Information sharing. In cybersecurity policy, "information sharing" is a hackneyed term. But it remains a fundamental component of any successful

---

[7] 2021 Verizon Data Breach Report, Figure 4 at 7, *available at* https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

cybersecurity strategy. The financial services industry has been at the leading edge. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is probably the most effective sector-based information sharing organization and serves as a model for other ISACs.

We have learned that effective information sharing is hard. For a long time, the focus has been on sharing technical indicators of compromise. Over time, it has become clear that the most useful information sharing is *actionable*, as close to *real-time* as possible, and separates *signal from noise.*

- Information is actionable if it can be used by network defenders to prevent or recover from a cyber incident. That often means not just technical indicators, but greater context about the threat actor and the tactics and techniques it may be using. So, for example, sharing a copy of a phishing email that a threat actor used to trick a user to click on a link and cause malware to be uploaded could be useful to other defenders who could try to detect and block similar emails before they arrive in users' in-boxes.

- The importance of timely information is clear: it does little good to share even actionable information if the malicious actor has already infiltrated a network and it is too late to act on the information.

- Prioritizing shared information can also help companies allocate resources. Companies often have a stream of information about potential threats, both from their own networks and from ISACs and from other sources. Given limited personnel and other resources, they may not know what information they should pay attention to and what they can safely ignore, or at least address later.

The cybersecurity industry and the government have made significant strides in improving information sharing. The Cyber Threat Alliance, for example, is a non-profit organization of more than 15 cybersecurity companies that enables near real-time, high quality information sharing among its members, which in turn benefits all of their customers. On the government side, the newly established Joint Cyber Defense Collaborative "will leverage CISA's broad authorities to share information about threats and vulnerabilities to enable early warning and prevent other victims from being attacked. This shifting paradigm will enable us to

transform information sharing into information enabling – timely, relevant, and actionable."[8]

One further step Congress should consider in connection with information sharing is mandating reporting of cyber incidents to the federal government. Such reporting is required in particular pockets, including by certain financial institutions that have a duty to report to regulators cyber incidents involving access to sensitive consumer information. But, as a general matter, no federal law requires companies to report cyber incidents to the government and, as a result, neither CISA nor any other government agency has a complete picture of what institutions have suffered cyber incidents, even in critical infrastructure sectors. Such information could clearly be valuable in bolstering cyber defenses: if, for example, reports started to come in about similar cyber incidents affecting a particular sector, CISA could warn others in that sector. Such information could be particularly valuable to smaller entities that may not be initial targets of a cyber attack campaign. Several bills are now pending before Congress that would require such reporting by critical infrastructure entities, and it should seriously consider passing such legislation.

Baseline Privacy Legislation. Instead of one comprehensive set of rules to protect personal and other data throughout the digital ecosystem, the United States has a patchwork of sectoral laws with varying protections depending on the type of data or the entity that processes the information.

One such sectoral law, the Gramm-Leach-Bliley Act (GLBA), applies to financial institutions. However, GLBA is inadequate to protect consumer financial data in today's world. It has at least two limitations:

- It applies only to "financial institutions," a defined term that does not capture the full range of fintech and other technology companies, data aggregators, and other entities that today collect and process consumer financial information. Recognizing this reality, the CFPB recently issued orders seeking to collect information from certain large technology companies "to better understand how these firms use personal payments data

[8] Testimony of Jen Easterly, Director, Cyber and Infrastructure Security Agency, before the Senate Homeland Security and Governmental Affairs Committee, Sept. 23, 2021, *available at* https://www.hsgac.senate.gov/imo/media/doc/Testimony-Easterly-2021-09-23.pdf.

and manage data access to users so the Bureau can ensure adequate consumer protection."[9]

Another set of entities that raises privacy and security concerns but may fall outside of GLBA are data aggregators, which offer financial services and tools by allowing individuals to consolidate account information from multiple financial institutions. Although these products can be useful, in at least some cases aggregators obtain customer credentials and collect their information through screen scraping, a practice that can raise significant security concerns.[10]

- GLBA is limited in its privacy protections: it focuses on providing notice to consumers of certain forms of data sharing and permits them to opt-out of some (though not all) of such data sharing. In so doing, GLBA places the burden of privacy protection on the individual and effectively adopts a default of broad sharing of consumer financial information.

The time has come for Congress to enact comprehensive federal privacy legislation that, particularly for sensitive information such as consumer financial data, shifts the burden away from consumers and imposes obligations on the entities that collect, use, and share data. We all know that consumers rarely read online privacy policies and that "notice and consent" therefore largely rests on a fiction. This model encourages companies to write permissive privacy policies and entice users to agree to data collection and use by checking (or not unchecking) a box. The sheer number of privacy policies, notices, and settings or opt-outs individuals have to navigate means that this model fails to provide adequate protection.

Privacy legislation should, among other things, require an entity to minimize the data it collects and processes based on the purpose for which the entity needs data (e.g., to provide a product or service requested by a consumer); prohibit unfair data

---

[9] CFPB, CFPB Orders Tech Giants to Turn Over Information on their Payment System Plans, (Oct. 21, 2021), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-tech-giants-to-turn-over-information-on-their-payment-system-plans/.

[10] CDT, Open Banking, May 2021, *available at* https://cdt.org/wp-content/uploads/2021/05/CDT-2021-05-25-Open-Banking-Building-Trust-FINAL.pdf.

practices, particularly the repurposing or secondary use or sharing of sensitive data without the express, opt-in consent of the consumer; and include data security requirements.[11]

Each of these steps will lower the risk to consumers from cyber attacks by reducing the amount of sensitive data that will be collected, stored, and shared, and ensuring that whatever data is collected is handled with appropriate care. Moreover, by providing a baseline that applies to all companies, comprehensive federal privacy legislation will avoid the situation we have today in which the same consumer data may receive some protection if processed by one company (such as a "financial institution" under GLBA), but less protection if processed by another.

Finding Points of Leverage in the Ecosystem. The cybersecurity approach in the United States depends on every entity, no matter how small, having at least some cybersecurity expertise. That model may not be feasible. We do not have the number of cybersecurity workers to staff every entity in the country. And, even if we did, as discussed above, smaller entities have limited resources and cannot realistically defend against sophisticated cyber actors. Information sharing, if done well, can help.

But we should also do more to look for places in the digital ecosystem where security improvements can have beneficial effects that propagate across the ecosystem. For example, key vendors in the financial system should be subject to direct regulation of their security practices. Although bank regulators have that regulatory authority, NCUA does not for vendors that serve credit unions. But security improvements by a commonly used vendor benefit all of its credit union customers.

More generally, we should consider whether other parts of the digital ecosystem provide opportunities to leverage broader security benefits. Improvements in software security, for example, will benefit all individual and business users of that software. Steps taken by an Internet service provider to block malicious traffic can have benefits that propagate to all of its customers. Whether through incentives or potentially liability, we should consider policies that will improve cybersecurity at key points in the ecosystem and thereby reduce the burden on individuals and smaller entities.

---

[11] These are not the only protections CDT believes should be included in federal privacy legislation. I focus here only on a few provisions particularly relevant to minimizing the harm to consumers from data breaches and other cyber incidents.