AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# CYBER THREATS, CONSUMER DATA, AND THE FINANCIAL SYSTEM

## HYBRID HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION AND FINANCIAL INSTITUTIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

NOVEMBER 3, 2021

Printed for the use of the Committee on Financial Services

**Serial No. 117–59**

U.S. GOVERNMENT PUBLISHING OFFICE
46–248 PDF WASHINGTON : 2021

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
CINDY AXNE, Iowa
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
RITCHIE TORRES, New York
STEPHEN F. LYNCH, Massachusetts
ALMA ADAMS, North Carolina
RASHIDA TLAIB, Michigan
MADELEINE DEAN, Pennsylvania
ALEXANDRIA OCASIO-CORTEZ, New York
JESÚS "CHUY" GARCIA, Illinois
SYLVIA GARCIA, Texas
NIKEMA WILLIAMS, Georgia
JAKE AUCHINCLOSS, Massachusetts

PATRICK MCHENRY, North Carolina, *Ranking Member*
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
ANN WAGNER, Missouri
ANDY BARR, Kentucky
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
BRYAN STEIL, Wisconsin
LANCE GOODEN, Texas
WILLIAM TIMMONS, South Carolina
VAN TAYLOR, Texas
PETE SESSIONS, Texas

CHARLA OUERTATANI, *Staff Director*

SUBCOMMITTEE ON CONSUMER PROTECTION AND FINANCIAL INSTITUTIONS

ED PERLMUTTER, Colorado, *Chairman*

GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
AL GREEN, Texas
BILL FOSTER, Illinois
JUAN VARGAS, California
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
RITCHIE TORRES, New York

BLAINE LUETKEMEYER, Missouri, *Ranking Member*
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
ANDY BARR, Kentucky
ROGER WILLIAMS, Texas
BARRY LOUDERMILK, Georgia
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee, *Vice Ranking Member*
JOHN ROSE, Tennessee
WILLIAM TIMMONS, South Carolina

# CONTENTS

# CYBER THREATS, CONSUMER DATA, AND THE FINANCIAL SYSTEM

**Wednesday, November 3, 2021**

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CONSUMER PROTECTION
AND FINANCIAL INSTITUTIONS,
COMMITTEE ON FINANCIAL SERVICES,
*Washington, D.C.*

The subcommittee met, pursuant to notice, at 10:06 a.m., in room 2128, Rayburn House Office Building, Hon. Ed Perlmutter [chairman of the subcommittee] presiding.

Members present: Representatives Perlmutter, Sherman, Green, Foster, Vargas, Lawson, Casten, Pressley, Torres; Luetkemeyer, Lucas, Posey, Barr, Williams of Texas, Loudermilk, Budd, Kustoff, Rose, and Timmons.

Ex officio present: Representative Waters.

Chairman PERLMUTTER. The Subcommittee on Consumer Protection and Financial Institutions will come to order.

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time. Also, without objection, members of the full Financial Services Committee who are not members of the subcommittee are authorized to participate in today's hearing.

I want to thank our witnesses for being here today. With the hybrid format of this hearing, we have some Members and witnesses participating in person and others on the Webex platform. For those of you on the Webex platform, we have had some trouble with the timer, so I will have to step in if people are running over their time limit. But we should be fine.

I would like to remind all Members participating remotely to keep themselves muted when they are not being recognized by the Chair. The staff has been instructed not to mute Members, except when a Member is not being recognized by the Chair and there is inadvertent background noise.

Members are also reminded that they may only participate in one remote proceeding at a time. If you are participating remotely today, please keep your camera on, and if you choose to attend a different remote proceeding, please turn your camera off.

Today's hearing is entitled, "Cyber Threats, Consumer Data, and the Financial System." Legislation noticed with today's hearing includes H.R. 3910, "the Safeguarding Non-bank Consumer Information Act;" a discussion draft entitled, "the Strengthening Cybersecurity for the Financial Sector Act," and a discussion draft entitled, "the Enhancing Cybersecurity of Nationwide Consumer Reporting Agencies Act."

I now recognize myself for 4 minutes to give an opening statement.

In both business and medicine, they have variations of what is known as the, "Sutton Rule." And for those of you who don't know what the Sutton Rule is, it is based on an old urban legend about a famous bank robber named Willie Sutton. When he was asked by a reporter why he robbed banks, Sutton casually replied, "Because that is where the money is."

The Sutton Rule suggests going after the obvious target. Banks and credit unions have long been targets for criminals, but today's criminals don't wield Tommy guns and they aren't only after cash. Cyber criminals also target financial institutions to steal consumer and business data, deploy ransomware, and disrupt services.

Ransomware attacks have been growing in frequency and severity for years. Over the first half of this year, there was a 1,318 percent increase in ransomware attacks on banks and credit unions.

Consumer financial and personal data is an attractive target for criminals. I doubt there is a person on this committee who has not had some of their personal or financial information exposed in a data breach. And I know I have been impacted by multiple data breaches over the last few years.

Tech companies, financial institutions, and many other businesses are collecting and storing more consumer data than ever before. The 2017 Equifax breach exposed the data of 147 million people, including 200,000 credit card numbers. And in 2019, Capital One was hacked and 100 million credit card applications were stolen.

The issues of cybersecurity and consumer data rights are intertwined, which makes cybersecurity critical for all financial institutions, large and small. Earlier this year, the CEOs of the largest banks in the United States testified before our committee. Congressman Huizenga asked them what was the greatest threat facing our financial system, or what was one of them, and the answers from four of the six CEOs included cybersecurity.

Similarly, in a recent survey, 71 percent of community bankers listed cybersecurity as a significant risk. Many financial institutions have strong cybersecurity protections, but such efforts don't come cheap. For some of the largest banks, cyber defenses cost more than a billion dollars per year.

In May of this year, President Biden issued an Executive Order on improving the nation's cybersecurity, to enhance information-sharing between the government and the private sector, modernize cybersecurity standards in government, improve software supply chain security, and make other improvements to cyber defenses.

Additionally, the Treasury Department recently announced new efforts to counter the rise in ransomware, including sanctions against cryptocurrency exchanges for facilitating ransomware payments.

The security and resilience of our financial system is not a partisan issue. Republicans, Democrats, and unaffiliated voters all share the desire to stop criminals from exploiting vulnerabilities and carrying out attacks on critical infrastructure, such as financial institutions.

I was pleased to work with my friend from Missouri, Ranking Member Luetkemeyer, on this hearing, and I appreciate his ideas and commitment to strengthening cyber defenses in the financial sector. And I also appreciate working with my friend, Representative Kustoff, on this very same subject.

I look forward to this discussion today to learn how we can work together to improve cybersecurity in the financial sector to protect businesses and consumers.

With that, I will now yield to the vice ranking member of the subcommittee, the gentleman from Tennessee, Mr. Kustoff, for 5 minutes for an opening statement.

Mr. KUSTOFF. Thank you, Mr. Chairman. Thank you for convening today's hearing.

And thank you to the witnesses for appearing today, both in person and virtually.

Without a doubt, our financial system is the envy of the world. I think we all agree with that. To make sure it stays that way, Republicans need to continue to embrace technology and support innovation. We do. In fact, both sides of the aisle do.

Private-sector innovation has led us to more dynamic and inclusive financial institutions that are better-equipped to serve American consumers, but bad actors continue to evolve. We have seen cyber espionage from foreign adversaries such as China, Russia, and Iran, and they have all spiked. And that is why it is crucial that we remain one step ahead.

Cyber attacks pose one of the greatest threats to our financial systems. And understanding what policies will better protect our financial institutions and consumers remains a top priority for this committee, again, on both sides of the aisle. As we have seen, there are vulnerabilities in the system, and they have to be identified and they have to be corrected.

We know that financial institutions have been one of the leading targets for cyber criminals. Just recently, we witnessed the Colonial Pipeline ransomware attack. Attacks of this size are more common than ever before. And with that, financial institutions are more mindful that a similar attack could happen to them.

We all know that such an attack could disrupt the flow of money to consumers, disclose closely-held personal information, and ultimately undermine confidence in the entire banking system.

So, again, I do want to thank the witnesses for being here today. They face the daily challenges of cybersecurity, and I think will provide us today with a real-world perspective.

This committee has already begun work on these important issues. We included bipartisan cybersecurity provisions in legislation just last year. And financial regulators are providing Congress with more information about cybersecurity risks.

In January of this year, Republicans issued a report which found that the COVID-19 pandemic and related relief programs created an environment ripe for cybercriminal activity, which continues to threaten our financial system and American consumers today.

As our economy recovers, protecting our financial system from cybercriminals assumes an even more important role. And we all know that technology is changing the way consumers and investors operate. Online commerce is becoming the norm, and people are

working from home more than ever before. Cyber exposure continues to grow. More work can and certainly must be done. Private-sector innovation, not government mandates, can lead the way. One-size-fits-all government policies won't be the solution.

With that, I do want to thank the chairman, and I also want to thank Ranking Member Luetkemeyer for convening this hearing, which I think will be both informative and helpful. I look forward to more bipartisan work on this issue.

And, Mr. Chairman, before I yield back my time, I would ask unanimous consent to insert Full Committee Ranking Member McHenry's remarks into the record.

Chairman PERLMUTTER. Without objection, it is so ordered.

Mr. KUSTOFF. I yield back.

Chairman PERLMUTTER. I thank the gentleman.

The Chair now recognizes the Chair of the full Financial Services Committee, Chairwoman Waters, for one minute.

Chairwoman WATERS. Thank you very much, Chairman Perlmutter, for holding this important hearing on cybersecurity.

Financial institutions have long been a top target for cybercriminals. Several years ago, Equifax experienced one of the largest cyber attacks, exposing the sensitive, personally identifiable information of nearly 150 million Americans. Government agencies and institutions are observing an alarming increase in the volume and sophistication of cyber attacks. According to one report, banks and credit unions experienced a 1,318 percent increase in ransomware attacks during the first part of this year.

So, I look forward to hearing from our witnesses on ways we can strengthen cybersecurity in the financial sector, including understanding how small institutions like minority depository institutions (MDIs) utilize third-party vendors to provide core processing and software, and what vulnerabilities arise from those partnerships that we need to address.

Thank you, and I yield back the balance of my time.

Chairman PERLMUTTER. The gentlewoman yields back.

It is now my pleasure to welcome each of our witnesses, and I want to introduce our panel.

First, we will begin with Samir Jain, the director of policy at the Center for Democracy and Technology, who is present in the hearing room today. Mr. Jain has decades of experience in private practice and government, including at the Department of Justice, and as a Senior Director for Cybersecurity Policy for the National Security Council.

Second, we have Mr. Robert James II, the president and CEO of Carver Financial Corporation. Mr. James is also the director of strategic initiatives at Carver State Bank, and currently serves as the chairman of the National Bankers Association.

Third, from my great State of Colorado, we have Carlos Vazquez, the chief information security officer of Canvas Credit Union in Colorado. Mr. Vazquez has decades of experience in information technology and security, and currently leads Canvas Credit Union's efforts in mitigating cybersecurity risks.

And finally, our fourth witness is Jeff Newgard, the president and chief executive officer of the Bank of Idaho. He is testifying on behalf of the Independent Community Bankers of America. Pre-

viously, Mr. Newgard was president and CEO of Yakima National Bank, and he is a graduate of the Colorado Graduate School of Banking.

Witnesses are reminded that your oral testimony will be limited to 5 minutes. I think our timer is now working. You should be able to see a timer on the desk in front of you or on your screen that will indicate how much time you have left. When you have 1 minute remaining, a yellow light will appear. I would ask you to be mindful of the timer, and when the red light appears, to quickly wrap up your testimony, so that we can be respectful of both the other witnesses' and the subcommittee members' time.

And without objection, your written statements will be made a part of the record.

I would also ask, just as a personal plea, to take your time with your testimony, and speak as clearly as you can, because, especially if you are on the platform, your testimony kind of reverberates in this room. So for these ears, I just would appreciate that.

Mr. Jain, you are now recognized for 5 minutes for your testimony, sir.

**STATEMENT OF SAMIR JAIN, DIRECTOR OF POLICY, CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT)**

Mr. JAIN. Thank you, and good morning. CDT is a nonpartisan, nonprofit 501(c)(3) organization dedicated to advancing civil rights and civil liberties in the digital world. On behalf of CDT, I appreciate the opportunity to testify today.

In my written statement, I discuss how the cyber threat environment has grown more dangerous. Two of you, I think, this morning, have already noted the statistic about a 1,318 percent increase in ransomware attacks in the last year.

Today, I am going to briefly discuss a few of the challenges that the financial services sector in particular faces in addressing cyber threats, and two potential areas in which we can make progress to better protect consumers and their data.

Even though the financial services industry has responded more proactively to cybersecurity challenges than most sectors, it still remains highly vulnerable.

I will focus on three particular reasons. First, financial institutions are highly-interconnected with one another and with third-party service providers, which has significant implications from a systemic perspective. A cyber attack can spread rapidly across the financial sector as an attacker moves laterally across institutions between financial networks. Moreover, if many financial institutions rely on a common vendor, a successful attack on that single vendor can have sector-wide consequences.

A second challenge is the gap between large and small financial institutions. The largest financial institutions have significant in-house cyber expertise and can develop or purchase sophisticated defensive products, but smaller financial institutions don't have those resources or capabilities. But they aren't immune from attack, just because they are small. In 2020, over a quarter of breaches involved small businesses.

A third challenge is the increasing reliance on technology. Today, customers interact with the financial system through networks,

even for traditional banking services. As a result, the financial sector is increasingly subject to disruption from cyber attacks. And that is all the more true once you look beyond traditional banks to the role of fintech, data aggregators, and large technology platforms.

In the face of these challenges, both the government and the private sector have sought to address cyber threats for a number of years, but much work remains to be done.

I will highlight two areas in particular. First, information-sharing remains a fundamental component of any successful cybersecurity strategy, but we have learned that effective information-sharing is hard. The most useful information is actionable. It can actually be used by network defenders to prevent or recover from a cyber incident. It also needs to be as close to real time as possible so that they can act on time. Any information-sharing needs to separate signal from noise. Otherwise, companies may not know what information they should pay attention to now and what they can safely ignore or leave for later.

One step Congress should consider in connection with information-sharing is mandating that critical infrastructure entities report cyber incidents to the Federal Government. Today, no government agency has a complete picture of what institutions have suffered cyber incidents, and such information could clearly be valuable in bolstering cyber defenses.

A second area to which Congress should look is baseline privacy legislation. Instead of one comprehensive set of rules to protect personal data throughout the digital ecosystem, we have a patchwork of sectoral laws with varying protections.

One such law, the Gramm-Leach-Bliley Act (GLBA), applies to financial institutions. However, GLBA is inadequate to protect consumer financial data for at least two reasons.

First, it applies only to financial institutions, a defined term that does not capture the full range of fintech and other technology companies and data aggregators that today process consumer financial information.

Second, 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. Yet, we all know that consumers don't read or rarely read online privacy policies, and that notice and consent, therefore, rests on a fiction. GLBA effectively adopts a broad default sharing of consumer financial information.

The time has come for Congress to enact comprehensive privacy legislation that shifts the burden away from consumers and imposes obligations on the entities that collect, use, and share data. 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 the data. It should prohibit the secondary use or sharing of sensitive data, without the express opt-in consent of the consumer, and it should include data security requirements.

Each of these steps will lower the risk to consumers from cyber attacks by reducing the amount of data that will be collected and shared and ensuring that whatever data is collected is handled with appropriate care.

Moreover, a common privacy baseline that applies to all companies will avoid the situation we have today, in which the same data may receive some protection if processed by one entity but less protection if processed by another.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Jain can be found on page 50 of the appendix.]

Chairman PERLMUTTER. Thank you, Mr. Jain. I appreciate your testimony.

Mr. James, you are recognized for 5 minutes for your testimony.

## STATEMENT OF ROBERT JAMES II, CHAIRMAN, NATIONAL BANKERS ASSOCIATION (NBA)

Mr. JAMES. Thank you, Chairman Perlmutter, Ranking Member Luetkemeyer, Vice Ranking Member Kustoff, Chairwoman Waters, and members of the subcommittee.

We appreciate the opportunity to testify this morning on cyber threats, consumer data, and the financial system.

My name is Robert James II, and I am the president of Carver Financial Corporation, the holding company for Carver State Bank in Savannah, Georgia. And I am also privileged to serve as chairman of the National Bankers Association (NBA).

The NBA is the leading trade association for minority depository institutions (MDIs). Our mission is to advocate for MDIs on all legislative and regulatory matters concerning and affecting our members and the communities we serve. Our members are on the front lines of reducing economic hardship in minority communities, which are underserved by traditional banks and have been the hardest-hit by the pandemic.

MDIs are critical economic development engines in minority and low-income communities, particularly due to our trusted relationships in these communities. Our internal teams work tirelessly to protect our systems and our customers from ever-evolving cyber threats. We take these threats extremely seriously. Unfortunately, our small scale and lack of access to cutting-edge technology does not always allow us to move with the speed or agility required at times like these.

A critical component of the resilience of the banking sector and its ability to assist underserved communities is the ability to adapt technologically. A host of different factors are intersecting to change the banking industry.

Like most community banks, MDIs are heavily-reliant on a handful of large technology companies that provide core processing services for the technological systems of our operations. These companies have no incentives to help us adapt to the changing competitive landscape. We are consigned to long-term contracts with punitive early termination provisions, cannot easily plug in modern outside solutions that make it easier for our customers to do business or secure their data, and the fundamental technology of many of these systems is antiquated and leaves us incapable of making rapid changes.

Because we are often the smallest clients of these giant firms, we receive the lowest priority for service. Our bank employees are con-

stantly training and monitoring our internal systems, but we do not get the latest and best technology from the big core processors.

We saw this play out during each round of the Paycheck Protection Program (PPP). Congress devised that program as a mechanism to aid small businesses who suddenly found themselves forced to close during stay-at-home orders, but a set of conditions favored larger businesses, and disadvantaged our banks in our communities.

Many banks only approved loans for existing customers, delayed the applications of sole proprietorships, and didn't allow enough time for institutions like ours to work with small businesses through the application process. This combined to shut out many minority-owned businesses.

Our banks found themselves sorely lacking in the technology needed to quickly respond. Unregulated companies were able to build technology solutions to address this market, but our banks, reliant on the core processors, were stuck with outdated processes that limited our ability to serve our customers.

We also need our regulatory partners to help. We need to invest more in technology and the right people to implement it, but these investments can result in criticism when their earnings don't meet regulatory expectations. We can also find ourselves in situations where local or regional examiners impede our ability to implement new technological solutions.

Several recent industry reports have attempted to detail how banks are responding to the challenge, whether through investment, data management, or new strategies to engage with customers. But with every step, there are obstacles, including potential workforce impact or just the burden of increased cost of technology investments.

Even as customers primarily conduct transactions over mobile, banks are discovering that they still expect branch service to be an option. Young consumers are also open to going to technology firms for all of their financial services. In a recent global survey, Accenture found that 31 percent of bank customers would consider Google, Amazon, or Facebook if they offered such services.

According to an FIS survey, the top 20 percent of firms are changing policy to promote and emphasize digital innovation. These firms are recruiting for digital technology expertise, encouraging more open innovation across roles, and appointing board-level roles with responsibility for digital innovation. It is difficult for our small banks to keep up.

In conclusion, cultural shifts inside the financial services industry, including the core processors and the regulators, are necessary to help MDIs and other community banks better orient ourselves to meet new customer demands.

Even though our teams are keeping our bank-side systems very safe, we are heavily-reliant on the big three core processors. Because of this concentration, our institutions are saddled with complex, onerous long-term contracts that stifle innovation in all areas, including security and identity verification.

As the smallest banks, we get the worst service, and are the last to get innovations. So, our banks have a hard time competing with large banks and cannot easily offer our customers the latest tech-

nology. Our regulators do not always allow us to make needed investments in technology because of pressure on earnings. These factors, when combined, leave our customers and communities frustrated and vulnerable.

We look forward to working closely with the committee and the subcommittee on ways we can level the playing field to ensure that our customers have access to the latest, most secure technology.

Thank you.

[The prepared statement of Mr. James can be found on page 59 of the appendix.]

Chairman PERLMUTTER. Thank you, Mr. James. I appreciate your testimony.

Mr. Vazquez, you are now recognized for 5 minutes for your testimony.

**STATEMENT OF CARLOS VAZQUEZ, CHIEF INFORMATION SECURITY OFFICER, CANVAS CREDIT UNION**

Mr. VAZQUEZ. Good morning, and thank you for inviting me to your subcommittee to discuss cybersecurity. We were provided with a few topics we would be discussing, so I would like to speak to these.

The National Credit Union Administration (NCUA) is seeking legislative authority to have oversight over credit union service organizations and third-party vendors that offer services to credit unions. The NCUA sits on the Financial Stability Oversight Council (FSOC), yet is the only Federal agency that currently does not have this statutory authority as it relates to vendors that serve banking organizations.

We believe credit unions deserve a Federal regulator with parity in this regard. Canvas Credit Union is supportive of parity for the NCUA, if the NCUA shares its information with State regulators and coordinates efforts with them whenever possible.

It is important that vendors who have access to our members' data are held to the same standards as credit unions. It is the responsibility of Canvas to ensure that our members' financial data is safe and secure. We expect no less from our vendors. An additional level of comfort would be possible knowing that our vendors would also be scrutinized by a regulatory agency complementing our own vendor due diligence programs.

On the efforts by government agencies to strengthen cybersecurity defenses, data-sharing is paramount in ensuring that credit union security departments are up-to-date in all threats affecting the security landscape. The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security (DHS), and the Financial Services Information Sharing and Analysis Center (FS–ISAC) are all doing a great job in disseminating threat information in a timely manner.

Security webinars, conferences, and summits all provide important security information which allows for credit unions to remain current with the constantly-evolving threat landscape.

In several recent summits, there was participation by CISA and Homeland Security as either guest speakers or presenters. Having these agencies present at these gatherings is very helpful and important, as the discussions presented provide vital information as

well as reassurance that our government is standing with financial institutions in their battle against malicious actors.

One service I would like to highlight is the automated network scanning tool provided by CISA. This free tool complements our tool chest for security systems that monitor and test our network. For Canvas, it is another tool to use, but for smaller credit unions, it could be the only tool they have. I would like to see more efforts placed on providing free services to help credit unions with their security frameworks.

Canvas Credit Union follows the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), as do many financial institutions. We are thankful for the guidance this provides on many architectures, such as zero trust and identity management. These guidelines definitely help credit unions in their roles of ensuring that our members' data remains secure.

FS–ISAC is a resource that provides collaboration tools and security education to member financial institutions. They do a fantastic job of ensuring that those who need help, get the help that they need.

On consumer data protection challenges, people and technology are the challenges that credit unions face in ensuring that our members' data is protected. Statistics show that a massive shortage exists in skilled security professionals, which are required to manage the sophisticated tools in use today. Many in the security industry are working to address this shortage by providing access to security training at all educational levels. We would expect our government would also be focused on addressing this skill shortage.

Technology will constantly be changing and improving to counter the threat landscape brought to us by the hackers bent on breaking into our networks to steal our data for their financial gain. Security teams are constantly on the defensive when it comes to protecting our networks. Security tools are improving, allowing for better detection to address vulnerabilities, but a focus by software vendors on security at the early stage of the development life cycle would ensure that most of these vulnerabilities are caught prior to going live with their product.

Vendors need to have a better focus on security of both software development and how they store our data on their systems. As mentioned before, vendors should be held to the same standard as credit unions when it comes to protecting our members' data.

In closing, cybersecurity will always be in a state of change. Yesterday, a threat was malware, viruses, or malicious executables inserted into our company's network. Today, as you have mentioned, ransomware, social engineering, and supply chain attacks are all threats today. And tomorrow, we will see the same, plus deepfake technology, and yet-unknown vulnerabilities in current hardware and software deployed by companies. Quantum process, which may allow for easy compromise of all of our current cyber technology is an added concern as well.

I would like to thank the subcommittee for bringing a focus on cybersecurity, the challenges it presents, and the role all of us have in protecting our data. It is an honor and privilege to speak with you today, representing Canvas Credit Union.

[The prepared statement of Mr. Vazquez can be found on page 73 of the appendix.]

Chairman PERLMUTTER. Thank you, Mr. Vazquez. I appreciate your testimony.

Now, our final witness, Mr. Newgard, is recognized for 5 minutes.

**STATEMENT OF JEFFREY K. NEWGARD, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BANK OF IDAHO, TESTIFYING ON BEHALF OF THE INDEPENDENT COMMUNITY BANKERS OF AMERICA (ICBA)**

Mr. NEWGARD. Chairman Perlmutter, Ranking Member Luetkemeyer, and members of the subcommittee, I am Jeff Newgard, president and CEO of Bank of Idaho, a $700 million asset community bank headquartered in Idaho Falls, Idaho, and serving markets throughout the State. I am testifying today on behalf of the Independent Community Bankers of America (ICBA), where I am Chair of the Cyber and Data Security Committee.

A community bank that does not successfully navigate cyber threats and safeguard its customers will lose their trust and cannot remain viable and independent. To enhance cybersecurity, we need support from policymakers in Congress, the Administration, and the agencies.

Community banks need to be on the cutting edge of technology to remain relevant and to compete with larger institutions as well as newer fintechs, but we need to adopt technology in a way that protects our vulnerable customers and the financial system as a whole. We operate in an ecosystem that includes all financial institutions as well as retailers, core providers, and many others. We are all in this together. An attack on any one node of the ecosystem is an attack on all of the participants.

Cyber threats have evolved in recent years from criminal attackers seeking profit to nation-states with massive resources and technological sophistication. The threats are greater than ever and continue to mount and evolve.

How do we manage the complexity? Ten years ago, community bank technology was mostly provided in-house. Today, this is simply an unaffordable option. Disaster recovery mandates as well as new technologies, such as internet banking, mobile banking, and imaging, have escalated the cost of cybersecurity.

In response, community banks have turned to core providers and other large third-party providers for their cybersecurity. At the same time, consolidation has occurred among the core providers. Today, just three or four providers dominate the market. This has increased their market power and leverage and, most importantly, it has put a target on their backs. Their connections to other institutions and servicers create a web of vulnerability.

What do we need from policymakers? While I provide more detail in my written statement, our recommendations form three broad themes. First, close the gaps in law, standards, and examination; second, create greater uniformity and harmonization of regulatory efforts; and third, promote sharing of information and best practices across the ecosystem.

The gaps in today's regulatory environment exist because not all parties that process and store sensitive information are subject to the Gramm-Leach-Bliley Act (GLBA), which requires safeguarding of sensitive data backed by examination to ensure compliance. Retailers and technology companies, for example, are not subject to GLBA. Core providers and other third-party providers as well as credit reporting agencies are not subject to examination.

A gap in accountability also contributes to systemic failures. When a data breach occurs, we believe that liability for that breach should be assigned to incentivize stronger security. The costs of a breach should be borne by the party that incurs the breach, be that a retailer, a credit reporting agency, or a bank or credit union. Too often, the breached entity evades accountability while financial institutions are left to mitigate damages to their customers.

Uniformity and harmonization will strengthen the ecosystem by eliminating redundancy, closing gaps, and strengthening weak links. Financial institutions are regulated, overseen, and examined by four agencies, which, unfortunately, do not adequately coordinate their data security efforts.

Thank you for the opportunity to testify today. My written statement provides comments on the legislation before the subcommittee today. And I look forward to your questions.

[The prepared statement of Mr. Newgard can be found on page 65 of the appendix.]

Chairman PERLMUTTER. Thank you, Mr. Newgard.

I would now like to recognize the Chair of the full Financial Services Committee, Chairwoman Waters, for 5 minutes for questions.

Chairwoman WATERS. Mr. Perlmutter, I would like to thank you again so much for this hearing today. And I want to thank you for the way that you have provided leadership on bipartisanship to deal with a serious issue confronting this country and this world.

I want to thank the witnesses who are here today, and I want to thank particularly, Mr. James, and of course, Mr. Newgard, whom we have heard from today. I am so very interested in all that we have learned about these core processors and the lack of competition and, of course, the cost to our smaller institutions, our minority depository institutions (MDIs), our Community Development Financial Institutions (CDFIs), and our community banks.

And I would just like to ask Mr. James whether or not you agree with Mr. Newgard? He not only gave us a very vivid description of what is going on, but he talked about recommendations, which I was very pleased to hear. Do you agree with the recommendations that Mr. Newgard just shared with us and is giving us more information about?

Mr. JAMES. Thank you for the question, Madam Chairwoman. Yes, I actually agree wholeheartedly with Mr. Newgard. As you stated, all of our community banks are really subject to the whims of a handful of very large companies. And while we are, in a sense, secure, additionally secure, because there are ways for us to cut off access to consumer information at our bank locations, and our staff at Carver State Bank, and I'm sure the staff at Bank of Idaho work tirelessly, and train constantly, to keep up with various threats and landscapes.

We are very dependent on these big core processors, and they have almost no incentives to work with our banks and make sure that we have the latest and greatest technology. I surmise that we are not necessarily getting the same level of service and attention that some of the larger institutions are getting, because we don't get the same level of service and attention when it comes to the customer-facing technology.

I do know that the big core processors are attempting to keep their systems very safe, but they present a significant amount of risk to the entire system, so I think that they need to be subject to examination. And I certainly agree with Mr. Newgard's recommendations.

Chairwoman WATERS. Thank you very much.

Mr. Chairman, just in this short period of time, I have heard enough from our witnesses today that leads me to believe that we must step up our action to deal with cybersecurity, particularly with our community banks, our CDFIs, and our MDIs, who are at the mercy of core processors who certainly attempt to do a good job, but I get the feeling that our smaller institutions are at the mercy of the work that is done for the larger institutions.

The other thing that I would like to say to my colleagues on the opposite side of the aisle is, I can't think of a better subject or project that we could work on together than cybersecurity. And I want you to know that I will join with you for whatever it costs for us to ensure that they are able to deal with the sophisticated cybersecurity that they need.

And, we really have to speed this up. We cannot linger as we deal with this, and then be forced to have to deal with the fact that there has been another big breach. We have to stop them, and we have to do it now. This is very important.

I appreciate working with the opposite side of the aisle. I don't always, but I do now. And I think this is a great opportunity for us to work together. Let's get busy. Let's do it quickly, and let's make sure that our smaller institutions have the resources that they need to do the job.

Thank you, and I yield back.

Chairman PERLMUTTER. I thank the chairwoman. And I appreciate the comments about how this is a subject that all of us need to tackle together.

And with that, I would like to yield 5 minutes to the ranking member of the subcommittee, the gentleman from Missouri, Mr. Luetkemeyer, for his questions.

Mr. LUETKEMEYER. Thank you, Mr. Chairman. And in the spirit of bipartisanship here that the chairwoman has set, before I begin my questioning, I want to take a moment to thank you for working with me in a bipartisan manner to hold this hearing today. I know we sat down and discussed the various topics to be able to find some common ground on, and this is one of them. And we were able to sit down and pick the subject as well as the witnesses. I appreciate your willingness to work across the aisle, and I am sure nothing last night had any sort of impact on what we are doing today.

But along these lines, Mr. Newgard, you mentioned a minute ago something about some of these different entities that could enable

the bad guy, so to speak, to access your records, and then the retailers or whomever escape liability for allowing the folks to access your records and documents and data.

Would you like to expand just a little bit and explain how that happens, and what the reaction is and the costs that are associated with it?

Mr. NEWGARD. Sure. Financial institutions are subject to examination, are subject to the GLBA. That does not go across the entire ecosystem. That is the issue. Retailers and the core processors are not subject to examination.

And what happens in the real world is when customers get their information breached, and say, for example, a debit card is compromised, we work very hard to get that account closed and reissued. There is very little incentive from the retailer or from the entity that was breached to help out in that process, because they don't bear any of the cost. In fact, many times, the consumer does not bear the cost. The bank or the financial institution has to bear that cost. So, there is very little incentive to work together to strengthen the entire system. And that is the important thing, that it is an ecosystem.

Mr. LUETKEMEYER. How do you resolve that situation? What is your suggestion on how you fix that? Do the courts need to step in here? Do the courts need to step in and assign blame, assign liability? Do we need to have contracts that somehow explain where the liability lies for certain actions when they are taken? How do you fix this?

Mr. NEWGARD. Yes. The retailers, the entities that are breached need to bear the cost. They need to be responsible for that breach. There is such a numbness within the consumer world. You hear about breaches all the time, and people are numb to it. There is no accountability. So, there needs to be a cost associated with having a breach instead of just assigning—they get out of it, basically. They sidestep it, and we are held accountable. In many cases, financial institutions have to pay for it.

And the consumer is numb to it. There have been cases where I try to reissue the debit card, but the consumer really likes the convenience and doesn't want to change cards. They would rather have the convenience of using their card.

Mr. LUETKEMEYER. Very good. Thank you. I have a limited amount of time, so I want to move on here.

Mr. James, I appreciate you being in front of us again. I always enjoy your comments. Thank you for being here.

The chairwoman made a comment today about the smallest banks being vulnerable. I know you represent a lot of small banks, and so I was curious as to a concern I have that the big banks seem like they have unlimited resources to be able to do whatever it takes to protect themselves. And the small banks are really vulnerable from the standpoint that they can only purchase the amount of protection they can afford. How vulnerable does that leave them?

Mr. JAMES. Thank you, Ranking Member Luetkemeyer. It does leave us vulnerable. I walked through our bank's cybersecurity program with our chief technology officer yesterday. And what he explained to me is that we constantly train, we constantly test our

employees. We constantly test our own systems that are sort of on the bank side. And because of the fact that we are plugged into these cores, we can cut off attacks at the local level and kind of minimize the damage.

The flip side is that it is very challenging if the core processor gets attacked. That could shut down our ability to provide our customers with access to their funds. That could shut down our ability to transact business for them. So, that is really where the challenge comes in, because of the vulnerability of the core processors.

Mr. LUETKEMEYER. So, what you are saying is that the big guys can afford their own core processor, while the small guys are at the mercy of the core processors, whomever they may be, that service their needs?

Mr. JAMES. Yes.

Mr. LUETKEMEYER. Thank you. I apologize. I am out of time.

Chairman PERLMUTTER. The gentleman's time has expired.

I will now recognize myself for 5 minutes for questions. And, Mr. Newgard, I was chuckling about your anecdote about the guy who didn't want to change his credit card because it was inconvenient. Recently, Wells Fargo notified me of some unauthorized charges, one in Ohio, and one in South Carolina. I said, okay, I will close my credit card and get a new one. And then, I realized all of the different accounts that were attached to automatic payments on that credit card, usually when they turned off my TV, or I didn't pay for the Terminex pest guys.

I can understand your customer saying they didn't want to change their card, because all of a sudden it really is inconvenient. So, we have to do our best to stop this at the beginning. But I did appreciate my bank notifying me of these unauthorized charges.

Mr. Vazquez, I have a question for you. In your testimony, you call for the National Credit Union Administration to have parity with other financial regulators regarding oversight of third-party vendors. What are some of the challenges credit unions face in vendor management, and how might expanding this authority benefit credit unions such as yours?

Mr. VAZQUEZ. Yes, sir. Thank you for that question. The credit unions, as others have mentioned—you have small credit unions, and you have large credit unions. And the larger credit unions can have a very robust vendor management program while the smaller ones cannot. And it takes a huge program to be able to look at the vendor, review their contracts, look at their stock and look at their security landscape to ensure that they have the security that we have to match.

So, what we are looking for is to say that we are being regulated to ensure that we are doing right by our members to hold their data safe and secure. Vendors that have our data that we contract with to better serve and provide services to our members now have our data, but they need to have the same security stance that we have. They need to have the same care that we have.

So without that type of regulation, we don't have that comfort, especially smaller credit unions, to know that we are all on the same level field in protecting our data.

Mr. PERLMUTTER. Thank you.

Mr. Jain, this question may be better suited to the Science Committee, but I am hoping you or any of the panelists might have an answer. Somebody mentioned quantum computing and the potential benefits or concerns that something like that might have.

In your studies, because you have had a pretty broad background, have you begun thinking about what quantum computing might do to enhance security or harm security?

Mr. JAIN. Thank you for that question. I think when we think about a lot of these new technological developments, whether it is quantum computing, whether it is the increased use of artificial intelligence, I think the difficulty is it can both help attackers and defenders, right? Because attackers can use these technologies, whether it is to try to overcome encryption or to automate their attacks and do them faster. On the other hand, defenders also potentially could take advantage of these technologies to help automate their defenses.

Although this is an area where I think this disconnect that we have been talking about between large banks and large institutions and small institutions again will come into play, because it is going to be the large banks that can afford to try to take advantage and deploy some of these newer technologies, and it is going to be much harder for the smaller institutions and banks. And so, I think this is just going to exacerbate the sort of divide that we are seeing between the large and the small banks.

Chairman PERLMUTTER. Thanks.

Mr. Jain, as we saw in the SolarWinds hack and other cyber attacks, criminals are increasingly attempting to breach service providers. And for minority depository institutions and community banks, if one of the core service providers was compromised, how many financial institutions might be affected, if you can give us a guess?

Mr. JAIN. Sure. Chairman Perlmutter, one of the beauties of the American financial system is the diversity of financial institutions and community-oriented financial institutions that we have to serve customers and create those relationships.

Our institutions really need to be able to protect our customers. On the banking side alone, there are probably 4,000 or so banks that would be vulnerable in the event of attacks on the big core processors. And that is probably 80 percent of the banks that are regulated that are ensured by the FDIC. That is my guess.

Chairman PERLMUTTER. Thank you, sir. My time has expired.

I would now like to recognize my friend from Oklahoma, Mr. Lucas, for 5 minutes.

Mr. LUCAS. Thank you, Mr. Chairman. I appreciate that.

Mr. Newgard, could you discuss how the COVID-19 pandemic has exacerbated cybersecurity threats, and what challenges your bank and others have seen as a result of the lost year, so to speak, which continues?

Mr. NEWGARD. The biggest challenge is the mobility of the workforce. Everybody, as was mentioned previously, went home and worked from home. That created a vulnerability, as people relied on working remotely. So, that has been a big challenge as people have adapted. And criminals take advantage of that and use that as an opportunity to create fraud, and there is incentive to do that.

Mr. LUCAS. Along that line, I guess I have to ask, is there anything that the government can do to help institutions address this kind of an issue? Is there additional flexibility or is there any way to help you cope with that?

Mr. NEWGARD. Yes, there are several, one of which is we talk about core providers, that we are at the whim of core providers and that it is very expensive. These contracts are expensive and they are long term. So if we go in, say, 2 or 3 years into a contract and determine that this is the wrong course of action for us, that there may be a better provider, it is very expensive to exit out of that.

If an examiner comes in and wants to weigh in on how that can be improved, it will take years for us to get out of the contract, and it is very expensive to do so. So, that is a big issue.

The other thing is, there are gaps within the regulatory environment. We have four regulators, and there is a lack of coordination between all four, and that provides an issue for the service providers as well, because they have four different regulators to try to cope with, and sometimes they are not in sync; they are at cross purposes. So, having harmonization within the regulatory environment would be helpful.

And then finally, more information-sharing across the ecosystem so that we can get ahead of these threats. We don't have Top Secret clearance, so we don't have information as it is becoming available through counterintelligence and all of the work we are doing on the government side.

We would like to have more information regarding vulnerabilities so that we can get ahead of it, because we feel like we are about a half-step behind in this area.

Mr. LUCAS. Mr. Newgard, continuing along this line of logic and a very important discussion, in your testimony you discuss that we should focus on creating greater uniformity among the financial regulators' cybersecurity standards.

Can you expand on this and, in particular, discuss what cybersecurity practices the Federal agencies now expect from you?

Mr. NEWGARD. Yes. We are regulated by the FDIC and the Idaho State Department of Finance. And there are other regulatory agencies out there, including the OCC and the Federal Reserve. So, what we comply with may not be what, say, Wells Fargo has to comply with.

And I am not saying that one-size-fits-all, but there should be some more harmonization so that we can have best-in-class regulation. And this is an area where we really need to step up and work together.

Mr. LUCAS. Mr. Vazquez, could you discuss the challenges in training employees to be prepared for cybersecurity threats?

Mr. VAZQUEZ. Absolutely, sir, and thank you for that question. Our employees, as with any other company's employees, are part of our security stack, as we would say. They are part of our tool chest. We know that they are highly-targeted.

In today's world, as I mentioned in my opening, social engineering is the easiest and fastest way for a malicious actor to get into our network. It is cheap for them to send a ton of emails that come through, and it just takes one click. It is amazing how a click al-

lows a malicious actor to gain a foothold in and then go lateral into our critical data.

It is super important that we maintain training for our employees, and we have done so. We test ourselves multiple times. We work with our learning department to ensure that we provide the materials to train our employees. We are sending out notices via our PSAs to remind them. We just went through the Cybersecurity Month, which highlighted the importance of cybersecurity and the role that our employees face.

Mr. LUCAS. Thank you. And thank you, Mr. Chairman.

Chairman PERLMUTTER. Mr. Vazquez, the gentleman's time has expired.

I now recognize the gentleman from Texas, Mr. Green, who is also the Chair of our Subcommittee on Oversight and Investigations, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. I greatly appreciate your hosting this hearing. And I thank the ranking member as well.

I am concerned about minority banks. I happen to have Unity National Bank in my congressional district. It is a small bank, but it serves a niche. And we want to do all that we can to protect all of our banks, especially these small banks that are helping communities that otherwise might not have the same opportunities to achieve their way of banking, because there is no bank in the community.

Here is my question: We talk about these breaches in the abstract, to a certain extent. We talk about the costs associated with megabanks having all of the technology necessary to protect themselves, whereas the smaller institutions, such as the $100 million, or very small banks—under $1 billion, you are a small bank; at $10 billion, you are still small.

My question is this: What is the amount of money that we are talking about for a small bank to properly acquire the technology necessary to protect itself? And I say this understanding that just for data acquisition to run the bank, I happen to have been told that it can cost around $50,000 a month. That is just to have the technology necessary to process the information that you receive to make sure that you can deal with the financial aspect of banking.

So, what does it cost? What are we talking about? I would like to get away from the abstract and save a lot of money and go right to a number. You don't have to be exact. Just give me some sense of it, please. I will allow whomever happens to have the necessary information to do so.

Chairman PERLMUTTER. Somebody jump in there.

Mr. JAMES. Congressman Green, I will attempt to address it first. You are correct in identifying the very, very steep cost of just the basic technology.

And so we have to think about it in terms of, the cost of the core processor is usually the second-largest cost on all of our balance sheets, our income statements, just behind people. And that is not including the people that it takes to run the technology. I would surmise that you are talking about a similar size investment in cybersecurity, which is really just going to be cost-prohibitive.

What would be a more interesting approach would be perhaps the regulators could actually help us. There are some innovative

things that are coming out of the FDIC. I heard the Chair of the FDIC just yesterday talk about the idea of having the FDIC actually pre-vet and do some vendor due diligence, on behalf of all community banks, on fintech companies and new technology providers, and essentially vetting those companies so that we know that we could plug into those companies safely and securely.

So if the regulators themselves could do something similar to what Mr. Newgard proposed, which is to coordinate amongst themselves but actually conduct a lot of this due diligence for our institutions, we would not only have the opportunity to increase the technology and improve the technology we are offering to our customers, but also to improve the security of that technology and keep up and compete with these large banks that just have basically unlimited resources to devote towards both technology and innovation and security.

Mr. GREEN. Thank you for your response.

Mr. NEWGARD. If I may, I would—

Mr. GREEN. Yes, sir, go right ahead.

Mr. NEWGARD. —add to that, is that the cost is really based on size and what other offerings you have. Do you have mobility? Do you have internet banking? There are all sorts of different add-ons that you can have with those core providers, so it is tens of thousands of dollars, and hundreds of thousands of dollars, in some cases. And the issue that you really hit on—

Mr. GREEN. Excuse me, if you don't own it but you are in a sense leasing it—

Mr. NEWGARD. Yes.

Mr. GREEN. —is that per month?

Mr. NEWGARD. We have to sign a contract for years.

Mr. GREEN. Yes, I understand.

Mr. NEWGARD. Yes.

Mr. GREEN. Okay, but I am trying to get some sense of what it is per month? What is it over the 10-year period? Give me more than it could be tens of thousands of dollars but not say per what amount of time.

Mr. NEWGARD. Yes. It really depends on the contract per bank, depending on how big it is.

Mr. GREEN. Well, give me a general number. Just assume you are doing all of the basics that you need. What would that be? Just basic banking.

Mr. NEWGARD. It is hard to say. It would be $20,000, I would say. But I can get you more information on specifically what the cost is to our bank.

Mr. GREEN. I would appreciate it. Thank you.

Here is why I would like to know. I want to make the argument that if we want to maintain smaller banks and keep them in business, the government is going to have to play a role in this. We are losing small banks at a rapid pace, and I want to do what I can to make sure that we do all that we can to protect them.

Mr. Chairman, thank you so much. You have been generous with the time.

Chairman PERLMUTTER. The gentleman's time is expired.

I would like to recognize Mr. Posey for 5 minutes, but I can't see him on the screen.

Mr. Posey, are you out—there you are.

Mr. POSEY. Yes.

Chairman PERLMUTTER. The gentleman from Florida is recognized for 5 minutes.

Mr. POSEY. Okay. Thank you very much, Chairman Perlmutter, for holding this hearing.

Mr. Newgard, cybersecurity looks something like other kinds of menaces that we manage through government action. For example, we have police forces to prevent crime and enforce deterrence, but we may expect people to behave rationally to avoid being victims of crime. In fire prevention, we may impose fire codes on individuals and businesses and also publicly provide a fire department to fight fires. In cybersecurity, we apparently impose regulations on financial institutions, and we also have agencies in government who fight cyber attacks and cybercrime and enforcement laws.

Are we achieving the right balance between regulating financial institutions and law enforcement to prevent cyber attacks and protect our financial institutions and the people that they serve?

Mr. NEWGARD. Yes, thank you. There needs to be more coordination between the police force, if you will, the regulators, and more harmonization so that we are getting the best-in-class approach to that policing, if you will. And then, it is not just us. That is the issue here, is that we are truly in an ecosystem where you can focus on just the financial institution, but you can have a breach.

And the criminals are going to go after the weakest link. So, they are going to go after the most unsophisticated customer or the smallest business to try to get in. And the retailers, the other fintechs, the screen scrapers, all of these entities are not subject to the same examination and regulation. So the police force isn't—they are ignoring that area where they are very focused on us, which is great, we embrace that regulation, but it needs to be throughout the whole ecosystem.

Mr. POSEY. Thank you. When a government agency like the Consumer Financial Protection Bureau (CFPB) imposes regulations on financial institutions to fight cyber attacks and cybercrime, we would expect that the agency would perform a cost-benefit analysis or a cost-effective analysis to ensure we are getting official regulation or at least minimizing the cost regulation. Can you please share your experience with us in that regard?

Mr. NEWGARD. The cost of the regulation?

Mr. POSEY. Yes. Does the CFPB look at alternative ways of regulating in this regard or to pick the most efficient way to achieve the goal or do they merely impose their preferred alternative without looking at other needs?

Mr. NEWGARD. I am not as familiar with them in particular. We are regulated by the FDIC and the Idaho State Department of Finance, and we have a great relationship with them. But they are, again, looking for more harmonization with the OCC and the Federal Reserve, to get best-in-class regulation.

Mr. POSEY. Yes. Looking at a broad array of cybersecurity issues, it looks like we have a number of Federal agencies regulating financial institutions to improve security. Do you believe it would make sense to have a single agency or a private-sector standards bureau to design the cybersecurity standards we impose on finan-

cial institutions? Would it help to make cybersecurity regulation more efficient and less redundant?

Mr. NEWGARD. Yes. Right now, we have a patchwork throughout all the States, and that becomes very problematic, so having standardization would be good. I would say that one size does not fit all institutions, so we do need to keep that in mind, that we are not the same as Wells Fargo. We have to keep that in mind, but having some standardization and harmonization would be great.

Mr. POSEY. One of the clear roles of government is protecting individual rights and especially private property rights. Without those protections, our market economy can't operate effectively, if it can operate at all. Is the Federal Government investing enough resources in cybersecurity countermeasures and law enforcement to adequately deter cyber attacks and protect our financial institutions and the public they serve?

Mr. NEWGARD. I think there is a tremendous effort on counterintelligence. Where I live, the Idaho National Lab has a great effort in that area. There is a lot of information out there, but it doesn't always flow down to the smaller banks and financial institutions. And I am a big advocate of sharing that information throughout our entire system and in a timely way. To learn a week later after a proposed attack is too late. We need to be much more timely on these issues.

Mr. POSEY. I see my time has expired. Thank you, Mr. Chairman, and I yield back.

Chairman PERLMUTTER. Thank you, Mr. Posey.

I will now recognize the gentleman from Illinois, Dr. Foster, who is also the Chair of our Task Force on Artificial Intelligence, for 5 minutes.

Mr. FOSTER. Thank you. And, Mr. Chairman, is it likely that there will be time for a second round of questions?

Chairman PERLMUTTER. I will talk to my counterparts over here, but yes.

Mr. FOSTER. If you could get us a reading on that, it would be great.

Many of our witnesses noted that small financial institutions are becoming increasingly dependent on third-party core processors. Credit unions in particular frequently rely on third-party technology providers for the processes that credit unions need, but these aren't cost-efficient to provide in-house, particularly for smaller ones. In some cases, however, these vendors might not follow the cybersecurity standards that are consistent with what is required of credit unions or they might not be familiar with the financial regulations concerning credit unions.

Now, once upon a time, the National Credit Union Administration (NCUA) had temporary authority to examine third-party vendors to address, in that case, the Y2K issue, but that authority expired in 2002. Now, recently, the NCUA, the Financial Stability Oversight Council (FSOC), and the U.S. Government Accountability Office (GAO) have all requested that this authority be reinstated for modern cyber threats.

My bill that is being noticed today, the Strengthening Cybersecurity for the Financial Sector Act of 2021, would simply make credit unions, Federal Home Loan Banks, and Government-Sponsored

Enterprises subject to the Bank Service Company Act, which would give the NCUA and the Federal Housing Finance Agency (FHFA) the same oversight of third-party vendors that bank regulators have for banks.

And I have to mention how gratified I am that at a time when it seems like nobody is able to get along with each other in Washington, that even above getting Democrats and Republicans to work together, we have been able to get the banks and the credit unions behind the support for this legislation. So, I am very grateful for that.

Mr. Vazquez, could you describe a little more about the need for stronger regulation of the service providers in this area, particularly in light of the increasing market concentration that we see in this industry?

Mr. VAZQUEZ. Absolutely, sir, and thank you for that. Everything you just mentioned we agree with, in that the NCUA should have greater authority to be able to regulate our vendors.

As mentioned before, and I think Mr. Newgard mentioned it, the vendors seem to have a playbook where they know a breach is coming. Breaches are coming so fast that it is almost—it doesn't affect us as it used to. A vendor now probably has a playbook to safely get a breach. All we have to do is wait for the next news cycle and it will go away. We will do a little bit of marketing to get our reputation back, and they move on. There is nothing that prevents them from doing so.

I think that to help at least with the credit unions, to ensure that we value our members' data, we want to make sure that nobody has access to that, we want to ensure that the vendors have that same feeling, that there is some kind of process for them to understand that if they have access to our data, it is not just a commodity to them to make money and to move forward, but that they need to protect that data as well as we protect the data.

Mr. FOSTER. Thank you. And is there a second level of sort of correlated risk that we should be worrying about? For example, the same way that a core provider can go down and impact many banks, if several core providers, for example, all use the same cloud service, they all use Amazon Web Services (AWS) or they all use SolarWinds, would the legislation we are proposing adequately cover the ability to look upstream and above just directly at the core processors but the people they are dependent on? Does it go all the way upstream, and is there a need for it?

Mr. VAZQUEZ. I think there is a need for that, and I will give an example. I believe Cloudstar was just a company that was victim of ransomware, and Cloudstar hosts in their systems many title companies as they do their business. We work with a title company that used Cloudstar. Because Cloudstar is a third-party vendor, we don't have access to Cloudstar to ask about our data that may have been on their systems.

So, we worked with our title company vendor to see if they were affected. They were. They had to rebuild from scratch everything that they had to do. But they could not provide us back what Cloudstar had, what Cloudstar went through, what Cloudstar data was affected.

Having more regulations upstream, as you mentioned, going to the third-party contractors would definitely help us ensure that we have the comfort of knowing that if a vendor that we contract with subcontracts out to other areas to have their data, that flow continues on.

Mr. FOSTER. Thank you. My time is up, and I yield back.

Chairman PERLMUTTER. The gentleman's time has expired.

The gentleman from Kentucky, Mr. Barr, is recognized for 5 minutes for his questions.

Mr. BARR. Thank you. Thank you, Chairman Perlmutter. I appreciate your leadership in holding this very, very important hearing.

And I appreciate the sentiments of Chairwoman Waters in talking about the need to tackle this in a bipartisan way. I think we can, and we should. It is overdue. This is a huge matter.

There has been some discussion about what is the right approach here, more harmonized regulation. I think there is a private-sector innovation point to be made. It is not black and white; it can be both.

But, Mr. Newgard, can you give us an example of some private-sector innovation that has made the financial system more secure from cyber attacks?

Mr. NEWGARD. Okay. Of course, our core providers, those would be private sector, and we really, as I mentioned before, rely on them for that innovation, almost solely. And the fintechs are coming online. That is private sector. By the way, we pay about—

Mr. BARR. Sorry to interrupt, but they are providing increasingly-innovative solutions for your institution?

Mr. NEWGARD. Yes, absolutely. We want them to do more in terms of innovation.

Mr. BARR. Let me ask you about regulation then. Are there regulatory requirements that cause institutions like yours, smaller banks, to shift more resources onto regulatory compliance rather than investing in cybersecurity and strengthening cybersecurity? In other words, are regulatory compliance burdens hampering your ability to invest in financial technology cybersecurity?

Mr. NEWGARD. Absolutely. The increased regulation makes it very difficult for small banks, and that is why [inaudible] to scale. That is why you are seeing banks consolidate.

Mr. BARR. Okay. Sorry, sir. Let me get into this issue of core processors. And I have heard this from my constituent community institutions, the take-it-or-leave-it kind of contract approach, that they express—vociferously they are expressing frustration with that. And I take seriously the suggestion, the recommendation from both you and Mr. James about harmonization of regulation and my colleague's legislation to bring these third-party vendors under supervision. I am open to that.

But my question is, the problem appears to be inadequate competition, so how do we get more competition in financial technology and among the core processors so you have greater choices of contracts for these services, which would not only bring down costs potentially, but also encourage greater private-sector innovation in this space? And is it a concern that more regulation on them could

potentially have the opposite effect of actually encouraging greater consolidation among core providers, which we don't want?

Mr. NEWGARD. Yes. We pay $51,500 that we budget a month in costs for our core provider with Fiserv. It is very expensive. We rely on them for technology, but the problem is, they don't keep up with innovation. So then, fintech comes in and provides that solution, but they are very unproven, very new, and they don't have the regulatory guidance, so they are at risk for cyber attacks.

Mr. BARR. But if I could shift over to Mr. James, because I am very sympathetic to the problem that MDIs and other small institutions face, in your testimony, you talked about needing to level the playing field. And my last question here is, how do we level the playing field for MDIs and small banks? I assume you are able to, through the Tax Code, deduct your investments in technology as a business expense, but, clearly, the economies of scale of your larger competitors puts you at a disadvantage. Besides the regulatory harmonization, what else would help MDIs and community banks level the playing field and access the technology you need?

Mr. JAMES. Mr. Barr, I think it is a great question. I think some of the answer there lies in regulation, but some of it does lie in competition and being able to access competitors to these companies. Oftentimes, what happens is when a good competitor comes along to one of the big core processors, they will go and buy that company rather than allow them to grow enough to be able to provide services to more of our institutions.

I think we really need to look at those contracts and we need to look at encouraging more competition so that we can move to different providers that are more flexible and more secure and provide our customers with better service.

Mr. BARR. Thank you. I yield back.

Chairman PERLMUTTER. The gentleman's time has expired.

The gentleman from California, Mr. Sherman, who is also the Chair of our Subcommittee on Investor Protection, Entrepreneurship, and Capital Markets, is recognized for 5 minutes.

Mr. SHERMAN. Naturally, this hearing is focusing on defending ourselves from cyber attack and hacking. We shouldn't just be focused on defense, but perhaps in classified sessions, focused on offense, especially when we are dealing with state actors or actors that are protected by states.

The U.S. has done little or nothing in this area. There was action taken against Iran's nuclear program that delayed it for a while by either Israel or the United States. Our intel community conjures up an image that they could make the lights flicker in the Kremlin or turn off the Internet Research Agency's operations in Saint Petersburg; they just choose not to.

I have no idea if that is correct, but I do know that Congress should be fully apprised of what are our offensive capacities, what could we do to develop them, and what should be our policies as to whether to threaten to use them or actually use them or maybe not.

Instead, we are here, as we are in many hearings, talking about a shield without ever talking about a sword. If we are not in a position to deter what some foreign governments are doing or delib-

erately allowing and encouraging, we are going to have an even bigger problem.

Turning to the private sector, we want to make sure the private sector spends more and does the best possible job. Basic economic theory says that the cost of a data breach should be imposed on those who could invest in safety measures and who should spend the appropriate amount of money and care in safeguarding data.

When Americans focus on the issues of this hearing, their first thought is on the big and well-publicized, and sometimes smaller and not well-publicized, data breaches where their personal information, particularly their credit card information, comes into the hands of ne'er-do-wells and criminals.

But our policy has been that if a big retailer has millions of credit card data files stolen, they don't face any liability. If it is a really big one, they may face some reputational risk, but all the costs are borne by the financial institutions.

Mr. James, would we get better investment by big retailers in safeguarding data if it was the retailers that had to pay the money that was occasioned by the breach?

Mr. JAMES. Mr. Sherman, I definitely think that you would see a renewed interest in protecting this data if some of those retailers, who were a part of this ecosystem that Mr. Newgard so eloquently described, bore some responsibility.

If our institution has a debit card that is breached or a checking account number that is breached, ultimately, we bear the responsibility for recouping that customer's funds. And those retailers that have—particularly very, very large retailers that have massive data operations are not really subject to any responsibility for protecting consumer data, certainly not the way that we are.

I certainly don't want to impose onerous costs on our small businesses, our small customers that are retailers, but even they are dependent on—

Mr. SHERMAN. I would just interrupt and say that the big hackers are not going after the small businesses. The treasure trove is in the big ones.

I do have a question for Mr. Vazquez. With regard to the question of expanding the National Credit Union Administration (NCUA) oversight of credit union third-party vendors, a primary concern is the risks with credit union service organizations (CUSOs). In your view, do these credit union service organizations and vendors pose the same level of risk to credit unions and customers? And if not, are there specific types of risks that would be more appropriate for NCUA oversight than others?

Mr. VAZQUEZ. Sir, I thank you for that question. And I do believe that they have the same type of risk. When a credit union such as Canvas partners with a CUSO or a vendor and we provide them our data so that our members can have a better service, we are basically—in some areas, people would think that we are transferring our risk to the vendor. And some people would think that we are now hands-off with that risk. We are expecting our vendor to take that risk. But, ultimately, that risk still resides with Canvas. That is our members' data. And we could try and transfer it, but it is really ours.

And we hope and expect that the vendors and the CUSOs that have our data would have maintain that same recognition of securing that data and have the same risk that we have.

Mr. SHERMAN. Thank you.

Chairman PERLMUTTER. The gentleman's time has expired.

The Chair will now recognize the gentleman from Texas, Mr. Williams, for 5 minutes.

Mr. WILLIAMS OF TEXAS. Thank you, Mr. Chairman.

We have seen a wave of new proposed regulations coming out of the Biden Administration that will cause banks to dedicate a significant amount of money towards new compliance costs. For smaller community banks, like the ones I deal with and most people, this means they will have less resources available to lend money into their communities or dedicate to cybersecurity efforts, and bottom line, it hurts Main Street America.

Whether it is asking banks to report account information from their customers to the IRS, or being forced to comply with a 900-page rule coming out of the CFPB on reporting small business loan information, these actions will force banks to divert significant amounts of resources—there is no question about that—because they have no clue what it is going to cost them.

So, Mr. Newgard, can you tell us how your bank has been adjusting with some of these potential new compliance costs coming down the pipeline?

Mr. NEWGARD. Yes. It is extremely expensive and it continues to ramp up. So, we are looking at hiring additional people to comply with things such as Bank Secrecy Act, and all of the other compliance burdens. And, simply, you have to get scale in order to be able to bear that cost. That is why you are seeing a tremendous amount of consolidation in our industry, because it is so expensive to comply, and the burden of the regulation continues to go up.

Mr. WILLIAMS OF TEXAS. Well, in the end, your customer is hurt.

As cyber threats are getting more sophisticated, there is a need for financial institutions to understand the threats and outages facing their third-party service providers. Unfortunately, I have heard from some of my market participants in Texas that the financial regulators are working on a new rule regarding computer incident notification requirements that could impose a significant new burden—here we go, a new burden—on community banks.

I understand the need to have transparency in the digital systems of the financial system to ensure that proper steps can be taken when something else goes wrong; however, I am concerned that the rule, as currently proposed, could both make community banks responsible for deciphering complex cyber incident notifications and cause market participants to share so much information with the regulators that they will not be able to determine what issues deserve attention.

Mr. Newgard, again, can you give us your thoughts on how we can strike the correct balance with cyber notifications so that banks can receive timely information from their service providers without creating an overly-burdensome review and reporting process for banks and, again, hurting Main Street?

Mr. NEWGARD. That's right. We already comply with good cybersecurity practices, and what we would ask is for harmonization

within the regulatory bodies, and then to spread that risk and liability to those that don't have it today: the retailers; the core providers; and the other people within the ecosystem. I will leave it at that.

Mr. WILLIAMS OF TEXAS. Okay. Lastly, I have talked with many different fintech firms in my district that have been dealing with a patchwork regulatory system of data security requirements coming out of different States. From my experience, what works in California, doesn't work in Texas. I repeat, what works in California, does not work in Texas.

Mr. Newgard, can you briefly discuss the benefits that your institution would see should a uniform data security standard come out of Washington? That is pretty scary.

Mr. NEWGARD. Yes. We are not in favor of a one-size-fits-all approach. We do need harmonization, I will stress that again, but definitely a one-size-fits-all approach doesn't work.

Mr. WILLIAMS OF TEXAS. Okay. So I would just say, in closing, as a business person who employs hundreds of people, and still has my business, that regulations hurt community banks, make them sometimes not competitive, and at the end of the day, affect your borrowers who are trying to grow their company and put more people to work. So, regulations do not help Main Street.

And with that, Mr. Chairman, I yield back.

Chairman PERLMUTTER. The gentleman yields back.

The gentleman from California, Mr. Vargas, is recognized for 5 minutes for his questions.

Mr. VARGAS. Thank you very much, Mr. Chairman. I appreciate very much this hearing, and I want to thank the ranking member also.

I have to say, though, there was a quip, stated something like, "what happened last night, of course, had no influence on the bipartisanship." I have to say, for me, zero, none, because I really don't like the Atlanta Braves or the Houston Astros, either one of those teams. Now, if it had been the Rockies or my beloved Padres that had won, well, then it is different. But since they weren't there, I really don't care too much about what happened last night.

Now, Mr. Newgard, I do want to ask you, you said that there is very little cost to the core providers when there is a breach. You also said the contracts are very expensive and they are only long term. The way the market is supposed to work is, if this is the case, there should be another actor that comes in, another participant with innovation to bring the cost down. Why hasn't that happened?

Mr. NEWGARD. The core providers are three or four. And, by the way, we pay about—we budget $51,500 a month for that service. So, we really push on those core providers to innovate, and many times they are slower than we would like them to be, and slower than our consumers and the small businesses would like to move.

So, that is where the fintechs come in. That is why we have a whole industry of fintech, because of innovation. The issue is, they are not subject to regulation like the GLBA, and the issue is they are startups, so they are brand new, and don't have much history—

Mr. VARGAS. I understand that, but I am asking why—in the core providers, why aren't there new startups there? In other

words, why isn't there competition? That is usually what happens in our market side.

Mr. NEWGARD. Yes. Mr. James stated this very well, that once one starts up, it is purchased, so it just becomes part of the whole. They don't even hardly let them get legs under them before they are consolidated.

Mr. VARGAS. Now, it has been interesting, because I think Mr. Barr, and certainly Mr. Williams and others have said, "We don't like regulation." And yet, a lot of the witnesses today seem to want to extend regulation to the core providers.

It has been fascinating to listen to what you on the private side have said tonight. Almost everyone says that the Gramm-Leach-Bliley Act (GLBA) should be extended, the Privacy Act should be extended, there should be harmonization. I assume you mean to make sure that the core providers, fintech, and everybody else has these regulations that they don't have now. Is that correct?

Mr. NEWGARD. That is correct.

Mr. VARGAS. Okay. Then I do, because we always have that fight that no regulation is good regulation. And we always think, well, no, you have to have regulations, then we just solve it. Going through this pandemic, a lot of banks didn't fail because we had some good regulations.

I do want to ask Mr. Jain, if I could, government information-sharing, you talked about that and said that we should have more of that and it should be actionable in real time. Could you comment a little bit more about that? Because we do spend a lot of money at the Federal Government level with respect to cybersecurity. What are we doing wrong?

Mr. JAIN. We have talked about information-sharing for many years, and I think we have learned that information-sharing or effective information-sharing is hard because it is not just a matter of sharing some isolated technical indicators.

What you really need is context and enough information in real time and actionable information that if a network defender receives the information, they can look at it, and they can say, oh, here is a copy of a phishing email that is being sent around that people are using to get access to people's networks. I can block that email, or I can look for that kind of email and block it.

Mr. VARGAS. Mr. Jain, I am going to interrupt you just for a second, because my time will run out. Why aren't we doing that? I understand that part. You told us that. Why aren't we doing that? Why can't we do that?

Mr. JAIN. I think we are getting there. I think it has taken us a while to realize that is what we need. And I think some of the innovations coming out of CISA, around the joint collaborating center that they just announced, I think is moving in this direction. But I think it is going to take more resources trying to get it economy-wide, and it is going to take time. So, I think we are moving in that direction, but we still need more time to get there.

Mr. VARGAS. Yes. I only have 4 seconds left. The only thing I would say is, "Go Padres!"

Thank you, Mr. Chairman.

Chairman PERLMUTTER. Okay. The gentleman yields back on that note.

And the gentleman from Georgia, Mr. Loudermilk, is here to talk about the Atlanta Braves, I will bet, but he is now recognized for 5 minutes.

Mr. LOUDERMILK. Mr. Chairman, I appreciate my colleague from California. And I understand that there was no California team good enough to make it to the World Series, so I understand why he was not affected by the game last night. But, "Go Braves! Go Braves, America's team!" And, by the way, Mr. Chairman, the Braves are in my district, so we are celebrating here today.

Chairman PERLMUTTER. Okay. The gentleman gets an extra 30 seconds because the Braves were in his district.

Mr. LOUDERMILK. Thank you, Mr. Chairman. I will use it wisely.

Cybersecurity and cyber threats is one of the issues that I have been working on since I have been in Congress. I spent some time in the military, in intelligence. Of course, security is a big issue for those in that field, especially protecting the data, the information that we have. I also spent 20 years running and owning an IT business, where, again, security was a main concern for our customers and we wanted to make sure that their networks were secure.

However, being here in Congress, I see that quite often, we will take one step forward and two steps backwards. Sometimes, we will go six steps backwards. I am going back to some of the basic tenets of what it means to secure data, and one of the primary tenets that we were taught in the military, and that I have kept throughout my businesses is this one principle: You don't have to protect what you don't have. You don't have to protect what you don't have, meaning, do not keep something that could be vulnerable just for the sake of having it.

And what we do here in the Federal Government, through mandates and regulations, and especially the idea that is being proposed right now for the banks to spy on everyone's bank account, and then all of that information by small institutions, large institutions, whatever is going to be sent to the Federal Government, which is, again, data that they don't need and they don't need to have.

And we have seen this continual flow of taking on more and more responsibility, the government either forcing businesses to keep data that they really don't need or forcing the businesses to send it to the Federal Government, which is a huge cybersecurity risk in itself, in my opinion.

So, I think we take one step forward and several steps backwards in trying to figure out better ways of securing data, where the bad guys are always going to be one step ahead of you, and when we really don't need to have this data to secure.

Another issue that I have been working on is the need for some type of uniform national data security breach notification standard. One of the issues is we have so many different standards throughout the nation that institutions have to comply with, various State laws, and those are often conflicting with the Gramm-Leach-Bliley Act and other Federal requirements, and it adds unnecessary complexity to the cybersecurity efforts, in my opinion.

So, Mr. Newgard, if banks were able to operate under a single set of rules, would that allow you to spend more of your time and resources defending against cyber attacks?

Mr. NEWGARD. Yes, having harmonization within the regulatory bodies would help significantly. And then voluntarily, we ask to share that breach information. And what we really need is to have more information shared from the government to us. I loved your comment about having too much data sent. That doesn't make sense. I think you are spot on there.

Mr. LOUDERMILK. That is one of the areas that we just tend to gloss over, and I have been bringing this up over and over in this committee, is that we keep talking about cybersecurity. We have put the onus on the businesses to be more secure, but then we require them to take more and more information, which they don't need to be taking. So, I appreciate that.

Another issue I have been focused on is payments fraud. Point-of-sale payments fraud has significantly declined, thanks to the adoption of chip technology, but the problem has shifted toward digital payments.

Mr. Vazquez, what are credit unions doing to enhance the security of digital payments?

Mr. VAZQUEZ. Thank you, sir, for that question. We partner with CO-OP Financial Services for our digital payments, and we work with them to ensure that they are monitoring for fraud. And we have a department ourselves that monitors for fraud.

Even though we spend quite a bit of money on my area, which is cybersecurity, we do spend the same amount of money in our fraud area to make sure that we have the right tools and the right people to monitor it. And it is important that the tools that we have are real-time tools, so that they are not a day old and the fraud that is happening isn't escaping while we are waiting for the information to come in. We are working with our vendors to ensure that the data we have is in real time so we can prevent the fraud.

Mr. LOUDERMILK. Thank you. I see my time is expired, so I will submit my other questions for the record. But thank you, Mr. Chairman.

Chairman PERLMUTTER. The gentleman's time has expired. And we should all applaud the Braves. They played a good game last night.

We have Ms. Pressley next, and then Mr. Rose, and then, if you wish, we will do a second round.

I am also going to make a suggestion that, Mr. Loudermilk, you get together with Mr. Foster and talk about this kind of stuff, because I think between the two of you, and after listening to this panel, we are going to have some good ideas as to what we should do.

So now, I would like to recognize the—

Mr. FOSTER. Mr. Chairman, Representative Loudermilk and I are already primary sponsors of some key legislation on digital identity.

Chairman PERLMUTTER. See? Okay, good. It is already working.

Mr. FOSTER. Your wish is our command.

Chairman PERLMUTTER. Okay. I would now like to recognize the gentlewoman from Massachusetts, Ms. Pressley, who is also the Vice Chair of this subcommittee, for 5 minutes.

Ms. PRESSLEY. Thank you, Mr. Chairman. You forgot to mention in my introduction, "and the Congresswoman for the Massachusetts Seventh District, proudly representing the Boston Red Sox."

Thank you, Mr. Chairman, for convening this important hearing.

Chairman PERLMUTTER. I apologize.

Ms. PRESSLEY. That's okay. Let the record reflect that.

But in all seriousness, through the first half of this year, banks and credit unions experienced a 1,318 percent increase in ransomware attacks, where attackers held private data hostage, and threatened to publish it should the victim not pay. You heard that right, 1,318 percent. So, this is a substantial and immediate threat to consumers in our financial system that really does require a substantial and immediate response.

The largest financial institutions devote tremendous resources to addressing cyber risk, yet smaller, regional, and community financial institutions don't have those resources or capabilities, even though cyber attacks on smaller institutions can also harm consumers and cause serious disruption. In fact, in 2020, over 25 percent of cybersecurity breaches involved were small business victims.

So, Mr. Jain, what sorts of challenges do financial institutions face in the prevention and detection of these attacks, especially when it comes to smaller, regional, and community financial institutions?

Mr. JAIN. Thank you for that question. I think they face a number of challenges. As we have talked about, they have significantly less resources, obviously, than the big players, both in terms of monetary resources to invest, but also in terms of access to in-house expertise. We have a shortage in the cyber workforce, I think, around this country, and so smaller institutions in particular, I think, have a harder time getting the in-house expertise they need.

The information-sharing, as we have talked about, is important. And while the big institutions are able to, for example, have people in the government centers that are designed for information-sharing, that is obviously not possible for the smaller institutions. And so, finding the right ways for information to get to smaller institutions in a way that is actionable in real time remains, I think, a challenge.

And then, I think, in many ways, smaller institutions have a greater dependence on vendors and other service providers because the big banks can provide a lot of these capabilities or develop them in-house. And as we have talked about, vendors create all sorts of security problems.

Ms. PRESSLEY. Thank you, Mr. Jain. And just building on that, I think that certainly makes the case for exactly why we need to address the fact that there are nearly 500,000 unfilled cybersecurity jobs across the nation. And this is why the Build Back Better Act makes these robust investments in cybersecurity workforce development with training opportunities at community colleges, Historically Black Colleges and Universities (HBCUs), and for our veterans.

The Biden Administration is partnering with private companies such as IBM, headquartered in my district, which is committed to

training more than 150,000 people in cybersecurity skills over the next 3 years, working with more than 20 HBCUs to build a more diverse cyber workforce.

Mr. Jain, just sticking with you for a moment here, how will these investments that I just enumerated help our nation combat growing cybersecurity risks in the financial services sector?

Mr. JAIN. I think it is crucial because, as you say, we do have a huge shortage of cybersecurity workers. And our system is set up where we are expecting every business, every small business to have that kind of cybersecurity expertise, and so that mismatch creates a real problem.

And, obviously, when you have that kind of shortage, just the basic law of supply and demand means that they can—cybersecurity workers can demand really large salaries, which, again, becomes a handicap for smaller institutions. So, I think there is no doubt that one part of this has to be to increase our cyber workforce.

Ms. PRESSLEY. Thank you, Mr. Jain. And before my time totally runs out, yes, these investments are certainly necessary to ensure that we have an equitable recovery to provide those good-paying jobs and to diversify this sector.

Transitioning to the issue of consumer justice and cybersecurity, under the Gramm-Leach-Bliley Act, covered financial institutions must inform customers of their data-sharing practices and allow customers to opt out of sharing their information with third parties. But most consumers, as you all know—we are consumers ourselves—don't have the time to read privacy policies and others may not understand the policy, or that they even have opt-out rights. So as a result, many of these folks are not opting out.

Mr. Jain, you argue that this opt-out system places the burden of privacy protection on the individual consumer and that the result of this shortcoming is that the GLBA effectively adopts a default of broad sharing of consumer financial information. So, how would you recommend that Congress change this data privacy burden so that more of it falls on the companies and not the consumer?

Mr. JAIN. Yes. I think we need to move away from this idea of notice and consent, that as long as consumers have notice, we have this fictional idea that they have consented, and start imposing some basic obligations on the entities that are collecting and processing this information, so among other things, to require them to only collect the information they really need to provide the product or service for which the individual signed up.

And if they want to use it for another purpose, then they have to come back to the consumer and say, hey, we want to share your data for this reason, is that okay? And if the consumer then expressly opts in, fine, but not sort of default to sort of, hey, we can hide this stuff in the privacy policy, and if you don't take the time to read it and check this box to opt out, we can do what we want.

Chairman PERLMUTTER. Thank you. The gentlewoman from Boston's time has expired.

Ms. PRESSLEY. Thank you.

Chairman PERLMUTTER. The gentleman from Tennessee, Mr. Kustoff, is now recognized for 5 minutes.

Mr. KUSTOFF. Thank you, Mr. Chairman, and thank you again for convening today's hearing. And thank you again to the witnesses.

And, Mr. Jain, thank you for personally appearing today. Mr. Jain, if I could ask you, going back to your prior life in government, both with DOJ and the National Security Council, can you compare and contrast, if you will, how the cyber threat environment has changed from the time you left the government to now?

Mr. JAIN. Yes. I think it has become more problematic. I think we are seeing an increased number of sophisticated cyber actors, not only nation states, but increasingly, criminal enterprises that have access to sophisticated capabilities. So, in that sense, it has become significantly more challenging.

We are also seeing more brazen attacks. Previously, 5 or 10 years ago, most of the attacks you saw were either things like denial of service or theft, whether it was of information or even money. But today, we are seeing so many more attacks that are actually disruptive, operationally disruptive, as we saw with the Colonial Pipeline and the likes, where they are really attacking critical infrastructure and really disrupting people's lives and basic services that people need. So I think in that respect, it has actually become a more serious problem for us.

Mr. KUSTOFF. And if I could, Mr. Jain, specifically about financial institutions, can you characterize how the threat or threats have changed during the time you left government to now as it relates specifically to financial institutions?

Mr. JAIN. Sure. One obvious change has been the rise of ransomware. I think a number of you have now mentioned the statistic about the 1,300 percent increase in ransomware attacks on banks. And that, in a financial institution context, obviously has major issues because it means that consumers, for example, may not be able to access their accounts or may not be able to use banking and financial services in a timely manner when they really need it. So, I think that is one example of where it has really had an effect.

And I also think it is important to recognize—we have talked a lot about the financial system as an ecosystem, but it is not only a financial ecosystem, but it is a broader ecosystem than that. For example, financial institutions rely on power, so to the extent that power companies and utilities are at risk for cyber attacks, that is going to have a downstream effect on financial institutions as well. And so, the risk to critical infrastructure broadly affects all companies, including in the financial institutions space.

Mr. KUSTOFF. Thank you, Mr. Jain.

And, Mr. Newgard, if I could maybe follow up on what Mr. Jain just talked about as it relates to the ecosystem, and, of course, you mentioned that interconnected ecosystem in your written testimony. Can you talk about that, and how an attack on big banks ultimately could filter down to smaller banks and community banks, et cetera?

Mr. NEWGARD. Sure. An attack on any financial institution, whether it be a large bank, whether it be a credit union or a small community bank, impacts significantly the overall financial system, and it hurts trust and it hurts communities.

Mr. KUSTOFF. Essentially, it is a domino effect. One attack on the large or larger banks is a domino to other banks down the ecosystem.

Mr. NEWGARD. That is right, certainly. But I would also say that an attack on a service provider, a core provider, if they get in there, if a perpetrator gets in there, look at how many community banks would be affected. We are talking about thousands of community banks and communities being affected by an attack on them as well.

Mr. KUSTOFF. So, not necessarily a direct attack on a community bank or a smaller bank, but from a best-practices standpoint, what could a community bank do to protect itself against attacks at larger financial institutions or banks?

Mr. NEWGARD. I would say having the harmonization of the regulators and also having those service providers be examined and have them be accountable to those requirements, because the bigger institutions have their own cores, if you will. They do a lot of this in-house, where we are reliant on third parties.

Mr. KUSTOFF. Thank you. My time has expired. I yield back.

Chairman PERLMUTTER. The gentleman yields back.

Another gentleman from Tennessee, Mr. Rose, is now recognized for 5 minutes.

Mr. ROSE. Thank you, Chairman Perlmutter and Ranking Member Luetkemeyer, for holding this hearing, and to our witnesses for being here with us today.

Unfortunately, cyber attacks across Tennessee and our nation are on the rise. While the ransomware attack that targeted the Colonial Pipeline, and the cyber attack on JBS in the meatpacking sector, have dominated the headlines this year, there have been countless other attacks affecting millions of Americans, and the financial sector in particular is routinely a major target of malicious cyber actors.

In order for our nation to meet the unique challenges posed by cyber attacks, it is essential that we have an adequate number of qualified cybersecurity professionals. However, it is becoming increasingly clear that there is a substantial shortage of qualified cybersecurity professionals in this country.

According to the data gathered under the Commerce Department grant, and as Representative Pressley just pointed out, there are nearly 465,000 unfilled cyber jobs in the United States. To help combat the shortage of cybersecurity professionals, the Department of Homeland Security and the National Security Agency have designated centers of academic excellence in cybersecurity.

I am proud to represent one such center of academic excellence in my district. The Cybersecurity Education, Research, & Outreach Center located at Tennessee Tech University in Cookeville, Tennessee, my alma mater, was established in 2015 in an effort to integrate university-wide initiatives in cybersecurity, education, and research.

One of the goals at the Tennessee Tech Center of Excellence is to help supply highly-trained students to the cybersecurity workforce. While I think we can all be appreciative of the work being done at Tennessee Tech to help fill these critically important jobs, there is clearly more work to be done.

Mr. Newgard, as the Chair of the Cyber & Data Security Committee at the Independent Community Bankers of America, would you talk a little about the challenges the financial sector faces when it comes to recruiting qualified cybersecurity professionals?

Mr. NEWGARD. This is a huge issue, and I would say that Governor Little from Idaho has created a cybersecurity task force to address some of these workforce issues.

This is bigger than we realize, because as the threat continues to increase, so does the demand for cyber professionals. We need more people. The issue within the financial institutions is our ability to pay for these talented people, because they get scooped up by other entities that are bigger and can pay larger salaries. So, it is a challenge to keep and attract good talent in the cyber area.

Mr. ROSE. Thank you, Mr. Newgard. I have spent my career in the IT training space, and have spent quite a bit of time through my own business helping to train cybersecurity professionals. And one of the old sayings we had in that industry is, if you train your employees—and you make reference to this—if you train your employees, they will leave you and go on to better opportunities. The only thing worse than that is not training them and having them stay. And I am sure, Mr. Newgard, you probably agree with that.

Mr. Jain, I would also welcome your input here regarding any challenges that you see when it comes to recruiting qualified cybersecurity professionals.

Mr. JAIN. Sure. As Representative Pressley alluded to, I think one of our challenges is making sure that we are drawing from our entire citizenry in terms of encouraging them to enter into the cyber workforce. We know that for a long time, for various reasons, women and girls have been more reluctant to get into technology. And we know that minorities sometimes don't see the same opportunities.

So, I think part of the solution to increasing the number of cyber workers that we have is making sure that we are doing everything we can to reach out and provide the opportunities really across-the-board to everyone, including underrepresented communities, because I think that is going to be critical in order for us to actually get the number of cyber workers we need.

Mr. ROSE. I am wondering, Mr. Jain and Mr. Newgard, if you believe that there is adequate credentialing or verification of the talents and capabilities of cybersecurity professionals today, or if you think there is more work to be done there? I mentioned the program at Tennessee Tech, but, historically, there has been some question about whether our cybersecurity professionals really know their stuff. Could you all comment on that in the remaining seconds we have?

Mr. NEWGARD. Sure. I am a big fan of certifications. I think certifications keep up quite well. We just need to have the workforce to do that, and potentially grants to help fund those.

Mr. JAIN. And I would just add in 2 seconds that I think it is also important to recognize that we shouldn't just assume that to be a cybersecurity professional, you need a computer science degree. I think we need to have different kinds of certifications and recognize that different kinds of skills can be useful.

Mr. ROSE. Thank you both.

I see my time has expired. And thank you, Chairman Perlmutter, for indulging me.

Chairman PERLMUTTER. The gentleman's time has expired.

The gentleman from Florida, Mr. Lawson, is recognized for 5 minutes.

Mr. LAWSON. Thank you, Mr. Chairman.

And I would like, again, to welcome everyone to the committee. This has been quite interesting. And I would like to thank Ranking Member Luetkemeyer also, because this issue is critical now.

My question is going to go to Mr. Newgard first. As you know, we are in an age where there is an increased reliance on technology, and with that comes an increased need to protect consumers' sensitive data. Financial institutions are pairing with technology services to provide other third-party vendors that are not versed in Federal regulations that protect consumers.

Based on your experience, do you believe programs that help close the gaps and establish digital cybersecurity infrastructure plans will be utilized by financial institutions?

Mr. NEWGARD. We are extremely reliant on third parties, and so anything that can make them more accountable is good. The other thing is, as part of this ecosystem, having retailers, core providers, everybody else within that ecosystem made accountable for consumer information and the liability associated with that as well. If they have a breach, they have to pay. That would go a long way.

Mr. LAWSON. Okay. Thank you.

And, Mr. Jain, it has been stated that cybercrimes could cost the world up to $10.5 trillion annually by 2025, which is right up the way. With cybercrime cases on the rise, how can Federal policy help aid and recovery for financial institutions that are victim to cyber attacks? Most of the proposed solutions today discuss preventive measures, but what action can we take to shape policy that would help mitigate the staggering effect of a data breach and help financial institutions effect recovery?

Mr. JAIN. Just to give a couple of examples, I think one thing that we should be thinking harder about from a policy perspective is whether there are points in the ecosystem where imposing requirements or requiring certain security practices can have benefits that sort of propagate across the ecosystem.

If you think, for example, of software providers or internet service providers, to the extent they up their security game, they eliminate a bug or a bug doesn't get into software, that has benefits that propagate across the whole ecosystem.

If you think of a program like Windows, when Windows has a problem, it affects everybody. But if we can fix it or we can create incentives so that commonly-used software providers or internet service providers who are serving tens of thousands of customers, if we can incentivize them to up their security game, that has benefits for everybody throughout the ecosystem.

So, I do think one thing that we should be thinking harder about is identifying those kinds of points in the ecosystem, what we can do there to improve security and sort of benefit everybody?

Mr. LAWSON. And the $10 million question that is always asked, Mr. Jain, is, what action could Congress take to improve cybersecurity and prepare to respond to attacks on the financial system,

which may impact the entire community and other sectors of our economy?

Mr. JAIN. One action, as I mentioned before, that I think Congress should take is to adopt Federal privacy legislation, because I think it really gets to a point that Representative Loudermilk made earlier, albeit from a different perspective, which is that if you have privacy legislation that, for example, requires providers to minimize the amount of data that they are collecting, minimize the amount of sharing that they do, that means there is just less data sloshing around the whole ecosystem so that if there, in fact, is a breach, there is less data that is being taken or fewer people's data that is being taken.

I actually think there is a really strong link between privacy legislation on the one hand, and reducing the negative effects of data breaches and the like on the other hand.

Mr. LAWSON. My time has almost run out, but I wanted to leave with you, is cybercrime international in scope with other countries now?

Mr. JAIN. Oh, absolutely. I think cybercrime is definitely international and requires international solutions for that reason.

Mr. LAWSON. Okay. With that, Mr. Chairman, I yield back.

Chairman PERLMUTTER. The gentleman yields back.

The gentleman from South Carolina, who is also the Vice Chair of the Select Committee on the Modernization of Congress, Mr. Timmons, is recognized for 5 minutes.

Mr. TIMMONS. Thank you, Mr. Chairman. I appreciate you holding this hearing. This is extremely important.

And I am just going to begin—I am actually not going to ask questions during my first 5 minutes, because I am going to take advantage of the second 5 minutes. But please listen to just how I am going to frame this.

In 2012, the Obama Administration proposed the Cybersecurity Act, that would largely address critical infrastructure. It failed. The Democrats at that time had a 58-seat majority. And the right didn't like it because it was overly prescriptive. It was too burdensome on businesses. And portions of the left didn't like it because of privacy concerns. It was too invasive.

So, let's talk about what has happened since then. We have had billions and billions of dollars worth of damage from cybersecurity breaches, both in the business community and in government: Epsilon; Target; Home Depot; Experian; T.J.Maxx; Sony; the Department of Veterans Affairs; and the U.S. Office of Personnel Management (OPM). They are increasing in number, and they are increasing in disruptive capacity.

Most recently, Colonial Pipeline, which affected my district, resulted in 75 percent of the gas stations in the Fourth Congressional District of South Carolina not having any gas. They did not have any gas. And I was getting calls all the time. And this is because they didn't have dual-factor authentication on their logins. So, this is basic stuff.

The EU passed the General Data Protection Regulation (GDPR) in 2016. A lot of people think that was overly prescriptive. It has created a lot of challenges. California has done the California Consumer Privacy Act (CCPA). That was in 2018. Colorado just signed

one into law in 2021. Legislation is currently pending in Massachusetts, New Jersey, North Carolina, Ohio, and Pennsylvania.

If we are going to try to do something in Congress: one, we are kind of late; and two, think about how challenging it is going to be. It would go through at least eight committees in the House, and probably five or six in the Senate. We don't need to just address the financial services component of cybersecurity and data privacy; we need to address the whole of the economy and the Government of the United States.

This is going to become increasingly problematic. And I know that we generally only legislate in crisis moments, but we have an opportunity to get ahead of that. And there are a lot of different ways you can try to craft legislation that would accomplish this objective, but I don't know if we have the will to do it because committee jurisdiction people are very protective of their committee's jurisdiction. There is a possibility of perhaps doing a joint select committee on cybersecurity.

We have to find a way to get everybody's buy-in before we—it needs to be a collaborative process, because the perfect will always be the enemy of the good, and we have to get the experts to write this legislation.

And it needs to be self-updating. We can't keep coming back and addressing every new development in technology. We don't have the ability—Congress doesn't do things like that.

So, we are going to get to the questions in my next 5 minutes, but one other thing I want to point out is preemption. What do you think the California delegation is going to do when we say that we are going to do away with the CCPA by Federal preemption, we are going to get rid of the law they have worked so hard on? They are going to go crazy.

But we can't have a patchwork framework of regulations. It would create such an incredible regulatory burden, such a compliance burden for your banks and your credit unions and for all of the businesses.

And I guess I am going to end with this: We are only as good as our weakest link. Small businesses or larger businesses that are breached, let's just use—we will go with Target or Home Depot. How much money do you think the banks had to spend to reissue tens of millions of debit cards? That is a compliance cost which is then passed along to the end users, to the customers.

This affects so many people. It affects every aspect of our economy, every aspect of our government. We are ill-equipped as a body to address it. We are running out of time.

So, that is the doom-and-gloom approach that I am going to begin with, and I am going to ask questions in the second round. But I look forward to you all weighing in on that assessment of the situation.

And with that, Mr. Chairman, I yield back.

Chairman PERLMUTTER. The gentleman yields back.

And to close out this initial round of questioning, we will have Mr. Torres from New York ask his 5 minutes of questions. Then, with the witnesses' indulgence, I assume that Mr. Foster and Mr. Timmons would like to ask some questions in a second round, and

anybody else—Mr. Lawson, Mr. Torres, you are welcome to do the same.

With that, I yield to the gentleman from New York City, Mr. Torres, for 5 minutes.

Mr. TORRES. Thank you, Mr. Chairman.

SolarWinds serves as a wake-up call about the vulnerability of the software supply chain. A malicious actor can target a computer network of a financial institution, not only directly, but also indirectly via the supply chain. So, we have a critical interest in securing the vulnerable supply chain that supports the financial system.

My first question is for Mr. Newgard. Big banks like JPMorgan can invest a billion dollars a year in cybersecurity. Do small banks have sufficient resources for cybersecurity, in your estimation?

Mr. NEWGARD. We do a very good job, I would say, as an industry. What we have done is relied on our core providers, because we simply don't have the ability to have all the redundancies and security at that level that the core provider does.

I have actually toured those facilities, those data centers, and they have very robust redundancies and security that we couldn't provide.

Mr. TORRES. Thank you. If I can just interject for a moment, what percentage of a small bank's budget typically goes toward cybersecurity?

Mr. NEWGARD. Just on the core side, we spend $51,500 a month, and that is just on our core provider. We have a whole department dedicated to cybersecurity and IT into the hundreds of thousands of dollars.

Mr. TORRES. And, Mr. Vazquez, same question for you. Do you feel credit unions have sufficient resources for cybersecurity, and what percentage of a credit union's budget, on average, goes toward cybersecurity?

Mr. VAZQUEZ. Yes, sir, thank you for that question. I feel I can answer the same. Credit unions, both large and small, are doing the best they can with the resources they have to mitigate the cybersecurity risks.

For us, I can't tell you exactly what the percentage is, but I can tell you that just our cybersecurity budget for tools that we need to ensure that our data is safe is close to a million dollars. That does not incorporate the cost of the employees, and as mentioned earlier, that cost continues to go up as we fight for the right resources to get the right people in to manage these sophisticated tools that we have.

A lot of smaller credit unions don't have the budget that we have. I am very, very thankful that our board and our executives are all bought in with cybersecurity and provide that budget for us to be able to buy the right tools, train our people, and ensure that we are doing the right thing.

Mr. TORRES. Mr. Newgard, you are the head of a bank, correct?

Mr. NEWGARD. CEO.

Mr. TORRES. Do you typically assess the cyber hygiene of your technology service providers before hiring them or doing business with them?

Mr. NEWGARD. Yes. We have an extensive vendor due diligence that we go through, and in the cyber area, we are increasing our

level of reliance on them. We just went to a managed Security Operations Center (SOC) with DefenseStorm recently, which is a cost, but gives us more security.

Mr. TORRES. Do you know if all of your technology service providers have a chief information security officer?

Mr. NEWGARD. Do I know if they have them? Yes.

Mr. TORRES. Do all of them have multi-factor authentication (MFA)?

Mr. NEWGARD. I couldn't answer that broadly. I don't have knowledge of all of the providers.

Mr. TORRES. Do all of those technology service providers have third-party assessments of their cybersecurity practices?

Mr. NEWGARD. I believe so.

Mr. TORRES. And, Mr. Vazquez, do you know if credit unions typically assess the cyber hygiene of their technology service providers before doing business with them?

Mr. VAZQUEZ. Yes, sir, we do. Fortunately, for Canvas, we do have a very robust vendor management program, and that allows us to query our vendors with contracts, ask for their SOC information, ensure that they are following the same practices that we expect them to.

To answer an earlier question, most do have MFA. Some still only have a single sign-on with using a password. And, obviously, we fight to have them change that, but not all vendors will do that. But, yes, we have them.

Mr. TORRES. My time has expired, and it might be easier said than done, but if I were a credit union or a bank, I would never do business with any service provider that did not have multi-factor authentication. That is the barest standard of cyber hygiene in the 21st Century.

I yield back.

Chairman PERLMUTTER. The gentleman yields back.

We will move to a second round. And, with that, I yield to the gentleman from Illinois, Dr. Foster, for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chairman.

I guess this is probably best for Mr. Newgard or Mr. Vazquez: Is the list of the market shares of all of the core processors publicly available? Are they well-known firms or are they sort of specialist firms? Just if you could, we will be asking—yes.

Mr. NEWGARD. Yes, they are pretty well-known. Fiserv is the one that we use, but there are about three others that dominate that area.

Mr. FOSTER. Okay. If you could respond for the record, just so we get a feeling who the big players are in that?

Now, Mr. James, Mr. Newgard, and others, you mentioned problems with the noncompetitive markets for core processors, partly due to a consolidation, but also due to vendor capture due to the high cost of switching vendors for core processing. This strikes me as very much like the market for electronic health records, which will effectively capture hospital chains or doctors' offices because of the high cost of switching over to a different competitor for these systems.

So, one of the things that we have attempted to do in Congress to make a more competitive operation is to have data portability

standards and interoperability standards so that it is more realistic to switch vendors on this.

Is there a need for something like this in this market, so you can make it a realistic threat to jump to a competitor? Have there been any discussions on this?

Mr. JAMES. I will jump in, Mr. Foster, and give you a quick example. We had one of our members, a Black-owned bank, that purchased another Black-owned institution that was not doing quite as well, and they just closed on the merger about 3 weeks ago.

The purchasing bank was on one core provider, and the target bank was on a different core. They had to pay $1.2 million to the target bank's core provider in order to move that data over to their core. And so, there is an enormous amount of cost.

So, if we could have some kind of consistency and data portability across these providers, that would really free up competition, because it is extremely onerous. Even if you wait until your contract is expired and you want to move to a new core provider, it is still going to cost you into the high six figures in order to do a conversion, which is one of the reasons why a lot of our banks end up staying with the same company over and over again for these long-term contracts. It makes us less competitive. It is very costly. And if we could have some consistency in standards, I think you would introduce more competition into the marketplace.

Mr. FOSTER. No, no, it is remarkable. There are markets where it is best that government just gets the heck out, like plain old internet, where we have said, okay, industry, figure it out, and any computer can talk to any other. But then there are markets, like electronic health records or apparently this market, where I guess the natural tendency toward monopoly is just so strong and toward vendor capture.

Many of you have also mentioned identity fraud and synthetic identity fraud, social engineering, and phishing attacks. And there is a pretty broad consensus that we have to get away from password-based systems to more secure systems.

There has been progress on this, including on the consumer-facing thing, with the rollout of Mobile ID, sometimes called digital driver's licenses, by many States. They were a standard that was developed by NIST, and iPhone and Android are now supporting them. It is a big part of their recent rollout of new updates to their operating system. And several States are rolling these out.

This allows you to essentially turn your cell phone into a security dongle that is associated with a REAL ID-compliant driver's license or other ID or a passport. And these things have the potential to really get rid of a lot of the agony that business and government sees with identity fraud.

Has the rollout in States gone far enough that you have really seen an effect of using these for Know Your Customer (KYC) requirements and so on, or is it still early days? Are any of you sort of aware of the use of this?

Mr. JAMES. Yes. We are generally aware of the trend, but it is still very, very early. I know in the State of Georgia, where our bank is located, we have not seen that yet. I am not sure about any of the other panelists, but it is still early days for us.

Mr. VAZQUEZ. Yes, sir. And I would agree with Mr. James that the technology is in its infancy. We are aware of it and are paying attention to it, because we do actually believe, as you just mentioned, that passwords are a huge area that allows for compromise. If we can take that away and move to something of what you have and get away from passwords, that would be the perfect solution. But right now, the technology is in its infancy. And as soon as it matures, we will definitely be looking at that to bring into Canvas.

Mr. FOSTER. Yes. I believe the technology is actually mature and—

Chairman PERLMUTTER. The gentleman's time has expired.

The gentleman from South Carolina, Mr. Timmons, is now recognized.

Mr. TIMMONS. Thank you, Mr. Chairman.

Mr. Jain, do you agree that Congress should preempt States and pass a comprehensive cybersecurity and data privacy framework for the U.S. economy?

Mr. JAIN. I definitely agree that Congress should pass that kind of legislation. I think on the preemption question, I would say two things. One, it is hard to answer the preemption question without knowing how strong the substantive protections are, because, obviously, if it is a really weak substantive privacy law, then that would, I think, mean that we wouldn't support preemption.

And the second point I would make is that I don't think preemption is an all-or-nothing thing. In other words, it is not we preempt everything or we preempt nothing. I think there are some laws, like you have referenced, like the California law and the Colorado law, which would be fairly parallel in some ways to a Federal privacy law where if it were strong enough, it may make sense to preempt.

On the other hand, there are other laws of general applicability that sometimes may read on privacy, whether it is civil rights laws that protect against discrimination or unfair and deceptive trade practice laws that deal with people who are deceptive in describing the privacy practices, where preemption, I think may not make sense. But I think there is room there to talk.

Mr. TIMMONS. Sure. I have concerns about Congress' capacity to craft such legislation. Not that we are not competent in many ways, but this is very challenging.

Do you think this is something that we could incorporate or ask NIST to take a first swipe at if we were to give them a general framework, to kind of work out some of the kinks on the front end and then maybe make it easier to go through the various committee jurisdictions?

Mr. JAIN. I would make two observations. One, there are actually quite few bills out there, both on the Republican and Democratic side, that I think are credible efforts, and sort of move us down this road.

I think it is quite possible that what legislation should do is to set forth basic duties and principles and then ask whether it is NIST or the FTC or some other regulatory agency, to try to fill those out and also, therefore, also be a little bit more nimble in sort of responding to new developments, as you noted earlier. But I

think there are some credible efforts that are already out there in terms of bills.

Mr. TIMMONS. Do you think a joint select committee would increase the likelihood of success of such an endeavor?

Mr. JAIN. I leave that to you, to some degree. I think the Commerce Committee in the Senate, and the Energy and Commerce Committee here in the House have, as I understand it, been taking the lead to the extent there has been activity around this. Whether that is sufficient jurisdictionally, I am not enough of an expert in congressional committee jurisdiction to be able to answer that.

Mr. TIMMONS. I have a feeling that the chairwoman of this committee might want to have a piece of the conversation in here. But the same can probably be said for a number of other committees, and that is the biggest challenge that we have.

Would you agree that GDPR and CCPA have perhaps gone a little bit too far in certain regards, and Congress should be careful not to take an overly-burdensome approach and perhaps try to facilitate some free-market solutions for enforcement mechanisms? I think one of the biggest challenges is growing government and creating standards when we are really just trying to facilitate best practices. What are your thoughts on that?

Mr. JAIN. I am not sure if I would characterize it necessarily as them going too far, so much as I would say that we need to move in a slightly different direction, which is that a lot of existing privacy laws focus on the idea of notice and then give consent on the part of consumers.

And as I talked about in my testimony, we all know that most consumers never read those 30-page privacy policies. And so, I think a privacy law that is based on the assumption that people are going to do that just doesn't really make sense and doesn't match with the real world.

What I do think we need to do is move more to a system in which we say, hey, there are some basic rules that if you are going to collect personal data, you have to follow. You have to minimize the data that you are going to collect. You shouldn't be sharing it in ways that are going to surprise consumers unless you go back and get permission, express permission from the consumers.

And you put those kinds of rules in place so that you can't bury in the privacy policy somewhere, hey, we are going to share this with these 10 parties. I think what we need to do is move in that direction, which I think is less about is GDPR going too far or too less, but sort of shifting the paradigm a little bit.

Mr. TIMMONS. Sure. I guess, last question: The U.S. economy is important, but the global economy also has an important role to play. What do you think about Congress trying to extend these protections to people abroad?

Mr. JAIN. We clearly have to pay attention to what is going on abroad, because most of our big companies obviously operate in multiple markets, and as a practical matter, it is very difficult for a large company to do different things, based on different geographies. That is why you see, for example, that a lot of companies follow GDPR sort of across the world, because it is just easier. Having implemented it, it is just easier for them to do that.

I think if it is going to be hard for Congress to pass a privacy law, I think it is probably hard to negotiate a worldwide privacy law. But having said that, I think paying attention and trying to figure out how what we passed works and meshes with laws in other countries is an important piece of this.

Mr. TIMMONS. Sure. Thank you for your time.

I yield back.

Chairman PERLMUTTER. The gentleman's time is expired.

Mr. Jain, one of the things we used to call the contracts you are talking about, we called them adhesion contracts, where the consumer really doesn't have much choice and has to adhere to whatever it was that the other contracting party was demanding. And here, it is people who haven't even read the contract, much less have much say as to how it is drafted.

I will now yield 5 minutes to the gentleman from New York City, Mr. Torres, for the last questioning. And I just want to thank the panel for allowing us to take extra time.

Mr. TORRES. Thank you, Mr. Chairman.

According to a report from Trend Micro, in the first half of 2021, there has been a 1,318 percent increase in ransomware attacks against banks and credit unions. According to suspicious activity report data from the Financial Crimes Enforcement Network (FinCEN), in the first half of 2021, the ransom amount paid out was $590 million, compared to only $416 million in all of 2020.

This question is for Mr. James. Mr. James, the internet has been around for a while. Cryptocurrency has been around for a while. What is driving this inexplicable explosion of ransomware, particularly against financial institutions?

Mr. JAMES. I think that it was mentioned earlier, Mr. Torres, that these bad actors are going where they find the money. And they are attacking what they think are vulnerabilities in our overall system. So, they are going to attack those institutions that they perceive as vulnerable and they are going to attack those systems that they perceive as vulnerable, particularly those that have the ability to pay.

And so our institutions, community banks, and minority depository institutions in particular, are being extremely vigilant about protecting our systems from these kinds of attacks, not only in terms of the amounts of money that we pay our core processors—at our institution, it is about $25,000 a month—but that all of the additional investments that we are making in training and people and consulting and infrastructure to try to keep up with the rapid rate of change and the rapid increase in these attacks.

Mr. TORRES. And do we know if the ransom payments are primarily coming from small banks or big banks? Do we know the distribution?

Mr. JAMES. I think it is primarily coming from larger institutions, rather than many of our members, but our members are being very, very vigilant and keeping aware of these situations.

Most of our institutions are carrying cyber insurance contracts, cyber insurance policies that would help to mitigate the cost. But the cost of the premiums of those contracts also is increasing exponentially, and we really need to be mindful of that cost as well as we face additional attacks in the ransomware space.

Mr. TORRES. It seems to me that one of the greatest challenges to cybersecurity is a lack of enforcement. Almost all crimes in cyberspace go unpunished, with less than 1 percent resulting in enforcement actions.

According to Third Way, for every 1,000 cybercrimes, only 3 of them will actually result in an arrest. Criminals are rational actors, so if the risks are low and the rewards are high, then cybercriminals have an incentive to commit cybercrimes in greater and greater numbers, at a faster and faster pace, and on a greater and greater scale.

And the data is crystal clear that cybercrime is on an exponential curve. According to Cybersecurity Ventures, the cost of cybercrime will go from $3 billion in 2015, to a projected $6 billion in 2021, to a projected $10.5 trillion in 2025. So, I am concerned about the trajectory of cybercrime, particularly as it relates to financial institutions.

Mr. Jain, I have a question about Section 1033. I am a strong supporter of Section 1033, but there are some legitimate concerns about cybersecurity and legitimate concerns about data aggregators, which tend to be largely unregulated and unsupervised.

How would you assess the state of cybersecurity with respect to data aggregators?

Mr. JAIN. I think there are some real issues there. In particular, I think what we have seen early on in the industry was the use of basically a technique called screen scraping, where essentially a consumer was turning over their credentials to the data aggregator, and the aggregator was scraping the information from the screen. And that clearly presented all sorts of security issues.

I think we are starting to move toward a system in which the data aggregators are communicating with financial institutions through application programming interfaces (APIs) or sort of interfaces designed for that, which I think is a positive step. Nonetheless, data aggregators, in general, don't fall within the purview, for example, of Gramm-Leach-Bliley, which sets sort of the privacy and security standards for other actors in the financial system.

So, I think it is important to impose privacy and security regulations on entities like data aggregators, ideally through, as we have been talking about, broad baseline privacy legislation, but short of that, then maybe bringing them within Gramm-Leach-Bliley at least as a transitional measure.

Mr. TORRES. Excellent. Thank you for the answer.

Thank you, Mr. Chairman.

Chairman PERLMUTTER. Thank you. The gentleman's time has expired.

I want to thank our panel for your expert testimony today. And we really do appreciate you giving us a little extra time. Obviously, this is a hot topic for all of us, one that we really need to try to get our arms around.

I think, as the chairwoman said, and as Mr. Luetkemeyer said, this is one area where there is a lot of common desire to minimize the attacks that we all face in the financial industry and elsewhere by cybercriminals and by nation-states and other bad actors.

So, thank you all very much for your testimony today.

I want to thank Mr. Thornton for putting these hybrid hearings together. It is not easy to have somebody in person and a number of folks on the platform, and it worked very well today. And I want to thank you for that, sir.

The Chair notes that some Members may have additional questions for these witnesses, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

And without objection, statements will be entered into the record on behalf of the following organizations: the National Association of Federally-Insured Credit Unions (NAFCU); the Electronic Transactions Association; the American Bankers Association; and the Credit Union National Association.

With that, thank you all very much. This hearing is now adjourned.

[Whereupon, at 12:39 p.m., the hearing was adjourned.]

# A P P E N D I X

November 3, 2021

**Opening Statement**

**Ranking Member McHenry**

**Date:** November 3, 2021

**Time:** 1 min (127 words)

---

Thank you, Madam Chair,

I appreciate the Chairman and Ranking Member for holding this hearing.

If you ask financial institutions and regulators what keeps them up at night – it's the threat of a cyber-attack.

This past December, I worked with my colleagues to enact legislation that will help this Committee understand what financial regulators and financial institutions are seeing and what they are doing to strengthen their cyber security platforms.

The Committee received the first installment of annual reports from four regulatory agencies in 2021.

The reports make clear that ransomware attacks and IT supply chain risks are urgent threats to the financial services ecosystem.

We should be using the Committee's resources to assess how regulators and industry are responding to these threats to protect the safety, soundness, and security of the financial system.

I yield back.


**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.

Testimony of Robert James II
Chairman of the National Bankers Association

Before the House Financial Services Subcommittee on Consumer Protection and Financial Institutions

"Cyber Threats, Consumer Data, and the Financial System"

November 3, 2021

Chairman Perlmutter, Ranking Member Luetkemeyer, Chairwoman Waters and members of the Subcommittee, good morning and thank you for this opportunity to testify on cyber threats, consumer data and the financial system. My name is Robert James II, and I am President of Carver Financial Corporation, holding company for Carver State Bank in Savannah, GA, and Chairman of the National Bankers Association (NBA). The NBA is the leading trade association for the country's Minority Depository Institutions ("MDIs"). Our mission is to serve as an advocate for the nation's MDIs on all legislative and regulatory matters concerning and affecting our member institutions as well as the communities they serve. Our member banks are on the front lines of reducing economic hardship in minority communities, which are underserved by traditional banks and have been hardest hit by the pandemic.

MDIs are critical economic development engines in minority and low-income communities, particularly due to our trusted relationships in these communities. Unfortunately, MDIs' small scale and lack of access to cutting edge technology does not allow them to move with the speed or agility required in times like these.

A critical component of the resilience of the banking sector and its ability to assist underserved communities is the ability to adapt technologically to meet customer demands. A host of different factors are intersecting to subtly, but distinctly, change the way the banking industry will operate in the near future. Our

banks, like most community banks, are heavily reliant on a handful of large technology companies that provide core processing services, or the technological systems of our operations. These companies have no incentives to help us adapt to the changing competitive landscape: we are consigned to long-term contracts with punitive early termination provisions, cannot easily plug in modern outside solutions that will make it easier for our customers to do business or to secure their data, the fundamental technology of many of these systems is antiquated and leaves us incapable of making rapid changes, and because we are often the smallest clients of these giant firms, we receive the lowest priority for service.

We saw this play out during each round of the Paycheck Protection Program. Congress devised the program as a mechanism to aid small businesses who suddenly found themselves forced to close during stay-at-home orders. A set of conditions that have favored larger businesses, including many banks only approving loans for existing customers, delaying the application of sole proprietorships, and not allowing enough time for institutions like ours to work with small businesses through the application process, shut out many minority-owned businesses. Our banks found themselves sorely lacking in the technology needed to quickly address the concern. Unregulated companies were able to build technology solutions to address this market, but our banks, reliant on the legacy core processors, were stuck with outdated processes that limited our ability to serve customers.

We also need our regulatory partners to help. We need to invest more in technology and the right people to implement it, but these investments can result in criticism when our earnings don't meet regulatory expectations. We can also find ourselves in situations where the local or regional examiners impede our ability to implement new tech solutions.

Demographic shifts are feeding new customer expectations as well, which are in turn creating an opening in the market for nonbank competitors and upstart firms. Industry observers now predict that within a decade, the biggest bank will be a technology firm.

A number of recent industry reports have attempted to detail how banks are responding to the challenge, whether through investment, data management or new strategies to engage with customers. But with every step, there are obstacles, including potential workforce impact, or just the burden of increased costs of technology investments.

Even as customers primarily conduct transactions over mobile, banks are discovering they still expect branch service to be an option. Young consumers are also open to tech firms for financial services. In a recent global survey, Accenture found 31% of bank customers would consider Google, Amazon or Facebook if they offered such services.

According to a FIS survey, the top 20% of firms are changing policy to promote and emphasize digital innovation. The report noted there are a number of steps being taken at leading firms in the past 12 months to accommodate digital innovation: 50% are recruiting for digital technology expertise; 43% said they were encouraging more open innovation across roles; and 39% were appointing board-level roles with responsibility for digital innovation.

In conclusion, cultural shifts inside the financial services industry, including the core processors and regulators, are necessary to help MDIs better orient themselves to meet new customer demands. We are overly reliant on the core processors and the space is dominated by three companies. Because of this concentration, our institutions are saddled with complex, onerous, long-term contracts that stifle innovation in all areas, including security and identify verification. Contracts are punitive if we want to terminate, and if we do, the extraction of our data for conversion is cost prohibitive and expensive.

As the smallest banks, we get the worst service and the innovations last. So, our banks have a hard time competing with large banks and cannot easily offer our customers the latest technology. This can leave our customers and communities frustrated and vulnerable. We know we don't have the latest and greatest customer facing technology from the cores. We also may not be getting the latest and greatest in terms of cyber security and consumer privacy. The National Bankers Association

and our members look forward to working closely with the Committee and Subcommittee on ways we can level the playing field and ensure that all of our customers have access to the latest, most secure technology.


Testimony of

**Jeffrey K. Newgard**

President and Chief Executive Officer

Bank of Idaho

On behalf of the

**Independent Community Bankers of America**

Before the

United States House of Representatives

Committee on Financial Services

Hearing on

"Cyber Threats, Consumer Data, and the Financial System"

November 3, 2021

Washington, D.C.

Chairman Perlmutter, Ranking Member Luetkemeyer, and members of the Subcommittee, I am Jeff Newgard, President and CEO of Bank of Idaho, a $700 million asset community bank headquartered in Idaho Falls, Idaho. I testify today on behalf of the Independent Community Bankers of America where I am Chair of the Cyber and Data Security Committee.

Thank you for the opportunity to testify at today's hearing on "Cyber Threats, Consumer Data, and the Financial System." This is a critical topic for consumers, community banks, and the broader financial ecosystem. A community bank that does not successfully navigate these issues and safeguard its customers will lose their trust and cannot remain viable and independent. To enhance cybersecurity, we need help from policymakers in Congress, the Administration, and the agencies.

**Our story**

The Bank of Idaho presently has 10 full service branches in operation across southern Idaho. In addition to retail and commercial banking, we also offer a full spectrum of trust and investment services, along with mortgage lending.

Recently named as a Forbes Best Banks in America, Bank of Idaho is committed to being the bank with a heart. That was exemplified in our PPP COVID-19 response lending, with over $100 million in Paycheck Protection Program loans to small business owners across the state. We have repeatedly been designated a top SBA lender in the state of Idaho.

My experience in community banking dates back over 20 years, and I have served as the CEO of two community banks in Washington State and now in Idaho.

The financial industry has evolved significantly in this time. Over the years, I've gained an increasing appreciation for both the promise of technology for reaching consumers and optimizing their experience and the threats that accompany technology. I've watched as major private sector institutions and government agencies have experienced cyber-attacks and seen the harm that it does to all system stakeholders – not only financial harm but reputational harm.

My interest has led me to become more deeply involved in financial technology policy through ICBA and other industry groups and to ultimately become chairman of the Cyber and Data Security Committee. My perspective reflects my interactions with literally hundreds of community bank leaders as well technology professionals throughout the financial ecosystem.

**Community banks and cybersecurity**

Community banks need to be on the cutting edge of technology to remain relevant and to compete with larger institutions as well as newer financial technology firms, or "fintechs." But we need to adopt technology in a way that protects our vulnerable customers and the financial system as a whole. Community banks operate in an ecosystem that includes all financial institutions – banks of all sizes, credit unions, and non-bank fintechs – as well as retailers, core providers, credit reporting agencies, data aggregators, and government agencies. We're all in this together. An attack on any one node of the ecosystem is an attack on all participants, including consumers.

The ecosystem continues to evolve. Notably, the rise of lightly regulated financial technology firms with less experience in cybersecurity has created more risk for the system as a whole. As technology has become more complex and pervasive, staying abreast of developments has led to hiring more technology professionals and demanded more of management's time and attention. Safely managing a community bank is more challenging than ever, but community bankers are committed to evolving because we recognize the critical role we play in our local economies.

**Extend Gramm-Leach-Bliley Act-like standards to close gaps in regulation and oversight**

The most secure parts of the financial ecosystem are those that are subject to the Gramm-Leach-Bliley Act. GLBA and its implementing regulations require financial institutions to safeguard sensitive data and provide for examination of financial institutions for their compliance with data security standards. Section 501(b) of the GLBA requires federal banking agencies to establish standards for protecting the security and confidentiality of financial institution customers' non-public personal information.

More specifically, the GLBA Safeguards Rule ensures that those under the jurisdiction of the GLBA have specific means to protect private information. GLBA requires "administrative, technical, or physical safeguards securing systems to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information." Notable requirements include employee training, proper software, and testing and monitoring of vulnerabilities.

In addition to protecting nonpublic personal information (NPI), organizations subject to GLBA must also take measures to detect and prevent as many instances of unauthorized access as possible.

Under current federal law, retailers, technology companies, and other parties that process or store consumer financial data are not subject to the GLBA federal data security standards and oversight. Securing data at financial institutions is of limited value if it remains exposed at the point-of-sale and other processing points. To effectively secure customer data, all participants in the payments system, and all entities with access to customer financial information, should be subject to and maintain well-recognized standards such as those created by GLBA.

**The importance of the core providers and other large third-party service and technology providers – and their vulnerability**

How have community banks managed the increasing complexity of technology? Ten years ago, community bank technology was mostly provided in-house. Today, this is simply an unaffordable option. In particular, disaster recovery mandates require expensive system redundancy. New technologies such as internet banking, mobile banking, and imaging have escalated the cost of cybersecurity.

In response, community banks have steadily migrated to core providers and other large third-party service and technology providers for their cybersecurity. At the same time, consolidation

has occurred among the core providers. Today, just three or four core providers dominate the market. Many community banks are customers of a single core provider. This has increased their market power and leverage, and most importantly, it has put a "target on their backs" for cyber disrupters. The core providers' vulnerability is our vulnerability because they store our customer data.

While community banks are diligent in their management of core providers and other third parties, mitigating sophisticated cyber threats against them can be challenging. Their connections to other institutions and servicers create a web of vulnerability.

Cyber threats have evolved in recent years from criminal actors seeking profit, to nation states with massive resources and technological sophistication whose goal is data gathering on our customers and businesses, systemic disruption, and political damage. Terrorist groups use cyber threats to fund terrorism. The threats are greater than ever and continue to mount and evolve.

Policymakers can help create a more secure financial ecosystem, mitigate threats, and help community banks by creating more manageable and harmonized regulatory standards, which in turn enhances security.

**Examination of the core providers and other large third-party service and technology providers**

Examination is a critical tool of ecosystem security and should create an umbrella which shields the entire system. I've noted the significance of core providers to community banks and the financial ecosystem. These providers, and all third parties, must not create gaps in supervision which increase risk to the ecosystem.

Regulators must be aware of the significant interconnectivity of these third parties and collaborate with them to mitigate risk. Effective, wholistic supervision should include additional regulation of core processors, fintech companies, and other third-party service and technology providers on which community banks rely. Supervision should evaluate the concentration risk relative to financial institutions. Employees of technology and service providers have access to confidential bank information that could be used to commit fraud, damage a bank's reputation, or compromise customer privacy. Regulators must ensure that these service providers implement nondisclosure and confidentiality requirements similar to existing regulatory requirements for banks. They must provide disclosure when employees or contractors are non-U.S. citizens or when data or systems are stored or run outside of the United States. We are only as secure as the people and businesses in which we put our trust.

**Examination and supervision of credit rating agencies**

Credit reporting agencies, which store a wealth of consumer data, are another point of vulnerability in the financial ecosystem.

The 2017 Equifax data breach demonstrated how important it is that the CRAs and other collectors/aggregators of customer financial data be subject to examination and supervision by prudential regulators. The release of this information has the potential to adversely affect

American consumers for the remainder of their lives and presents unique challenges for all financial institutions in authenticating new and existing customers. Subjecting CRAs and similar organizations to appropriate oversight may prevent future breaches.

Credit reporting agencies also have a significant role in fighting synthetic fraud and reducing or eliminating the prevalence of credit score manipulation, which is perpetrated using many of the same, well-known techniques used in synthetic fraud.

**Governmental departments and agencies**

Despite issuing cybersecurity regulations and guidance covering financial institutions, governmental departments and agencies have also been subject to data breaches. The government has a responsibility to safeguard sensitive information. Liability and costs of a breach of governmental systems may be unfairly assigned to the banking sector and result in a loss in confidence. Additionally, there is high risk of identity theft of American citizens.

**Data security**

Data breaches at credit bureaus, retailers, hotel chains, social media networks, and elsewhere jeopardize consumers' financial integrity and confidence in the financial services industry. Community banks are strong guardians of the security and confidentiality of customer information as a matter of good business practice and legal and regulatory compliance. Safeguarding customer information is critical to maintaining public trust and retaining customers. However, bad actors will continue to look for weaknesses in the payments and information systems in various industries, and breaches will occur.

What happens in the wake of a breach will determine how damaging it is. Consumers should be promptly notified of breach so they can take steps to protect themselves from identity theft and harm to their credit.

ICBA supports a national data security breach and notification standard. Many states have enacted laws with differing requirements for providing notice in the event of a data breach. This patchwork of state notification laws and overly broad notification requirements only increase burdens and costs, foster confusion, and ultimately are detrimental to customers. Federal banking agencies should continue to set the standard for financial institutions.

To protect their customers, banks need timely and enhanced breach notification. Community banks must receive timely notification concerning the nature and scope of any breach that may have compromised customer information so that they may take steps to mitigate any damage. Enhanced breach notification can save community banks time and money and is in the best interest of customers. Technology and service providers should also, as a matter of course, provide visibility into their business continuity, incident response, and other critical resiliency plans.

Breach liability should be assigned to incentivize stronger security. Regardless of where a breach occurs, as stewards of the customer financial relationship, banks take a variety of steps at their own expense to protect the integrity of customer accounts. However, these costs should ultimately be borne by the party that incurs the breach. Barring a liability shift, community banks should have access to various cost recovery options.

Too often, the breached entity evades accountability while financial institutions are left to mitigate damages to their customers.

**Need for uniformity in data and cybersecurity regulation**

Financial institutions are regulated, overseen, and examined by four agencies: The Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the National Credit Union Administration. Unfortunately, these disparate agencies do not adequately coordinate their data security efforts. Achieving greater uniformity and consistency among these agencies should be a priority. Uniformity and harmonization will strengthen the ecosystem by closing gaps and strengthening weak links. It will also ease compliance by creating greater clarity into what is expected of a financial institution. When compliance is less burdensome it is more effective in achieving its goal: a more secure financial system.

**Examiners should act as partners in cybersecurity**

Examiners have invaluable knowledge of industry best practices through their examination of numerous institutions. A partnership mentality in examination would be of great value in enhancing system-wide security.

For example, examiners review community bank contracts with our core providers and provide valuable insight into contract terms. We appreciate their guidance. Unfortunately, because these contracts typically last from three to seven years, we don't have the opportunity to act on examiner guidance until the next contract renewal. I would urge examiners to play a more proactive role in this regard by reviewing contracts before they are signed and providing guidance throughout the contracting process. This practice would strengthen our contracts and better protect our customers.

**Sharing of information and best practices will promote security**

Looking beyond the partnership between examiners and financial institutions, ICBA supports voluntary information sharing among financial institutions of all sizes, public-private partnerships, and federal agencies for the purpose of identifying, responding to, and mitigating cybersecurity threats and vulnerabilities while appropriately balancing the need to secure customer information.

The sharing of advanced threat and attack data between federal agencies and financial sector participants helps manage cyber threats and protect critical systems. ICBA supports community banks' involvement with services such as the Financial Services Information Sharing and

Analysis Center (FS-ISAC), a non-profit information-sharing forum established by financial services industry participants to facilitate public and private sector sharing of physical and cybersecurity threat and vulnerability information. ICBA supports FS-ISAC's cross-sector information sharing efforts to enhance overall resiliency of the nation's critical infrastructure. ICBA's Sector Fraud Working Group shares fraud intelligence with a wide range of public and private stakeholders.

We must ensure that best practices are shared as well. We compete for customers by providing better products, services, and relationships, but we should all cooperate in preempting threats and strengthening cybersecurity. The ecosystem is only as strong as its weakest link.

ICBA is hopeful that the Cybersecurity and Infrastructure Security Agency's (CISA's) recently announced Joint Cyber Defense Collaborative (JCDC) will result in more effective sharing of threat information and best practices. JCDC will coordinate with partners from the federal interagency, private sector, and state, local, tribal, territorial (SLTT) government stakeholders "to drive down risk before an incident and to unify defensive actions should an incident occur," according to the CISA website.

We hope that community banks will have a seat at the table since not all risks apply equally between large and small banks and what is an effective mitigating strategy to improve cyber security for one, might not be the answer for the other. Gaps in security and training must be identified and addressed with dedicated governmental resources for community banks to ensure that community banks are adequately prepared and can actively participate in the defense of the financial sector.

**Legislation before the committee today**

We appreciate the opportunity to share our perspective on bills before the committee today.

**H. R. 3910, The Safeguarding Non-Bank Consumer Information Act (Rep. Lynch)**

This bill modifies GLBA and increases regulation of data aggregators and will require them to better protect customer data. ICBA is concerned, however, that the expansion of CFPB's rule making authority over banks would be duplicative since banks are already regulated by the OCC, FRB, or FDIC for the protection and privacy of their customers' data and information. In particular, we recommend revising the bill's definition of "data aggregators" to ensure that it covers non-financial institution data aggregators that provide information to other non-financial institutions and/or individuals. We are happy to work with Rep. Lynch to strengthen this bill.

**The Strengthening Cybersecurity for the Financial Sector Act (Rep. Foster)**

This bill would partially close a loophole that has allowed credit unions to outsource their information technology and other services to Credit Union Service Organizations (CUSOs), to avoid regulation of those services and activities. This is an important change which ICBA supports.

However, ICBA would support additional legislation to allow NCUA to directly examine and regulate CUSOs, core providers, and other large third-party service providers. This would correct a disparity in rulemaking between banking regulators and credit union regulators and strengthen the financial sector as a whole. Effective cybersecurity must include visibility, harmonization, and cooperation.

Current law results in less oversight and visibility into CUSOs and potentially a more relaxed security posture and greater vulnerability for them.

**Enhancing Cybersecurity of Nationwide Consumer Reporting Agencies Act**

ICBA supports this legislation. It would amend the Fair Credit Reporting Act to provide that CRAs are subject to cybersecurity supervision and examination by the CFPB, including section 501 of the Gramm-Leach-Bliley Act. The Act would address a vulnerability in the financial ecosystem which we have discussed in this statement.

**Legislation outside the jurisdiction of House Financial Services**

**The Cyber Incident Reporting for Critical Infrastructure Act of 2021**, a bipartisan amendment in the House-passed National Defense Authorization Act (Reps. Yvette Clarke and John Katko)

This legislation would address several of the concerns discussed in this statement.

- The bill would enhance public-private information sharing through the creation of a Cyber Incident Review Office to receive, aggregate, and analyze reports submitted by covered entities to enhance cybersecurity awareness of threats across critical infrastructure sectors and publish quarterly public reports describing its findings and recommendations.
- The bill would consider existing regulatory reporting requirements in efforts to harmonize cyber incident reporting. Currently, community banks must report such incidents to their primary regulator, to FinCEN through Suspicious Activity Report (SAR) filings and share information with the Financial Services Information Sharing and Analysis Center ("FS-ISAC").

However, ICBA has several concerns about this legislation and recommendations for clarifying and strengthening it. These recommendations concern the timeline for reporting cyber incidents, the scope of what must be reported, the scope of information reported, exemptions for information already reported to financial regulatory agencies, protections against legal liability for incident reports, and penalties to which community banks would be subject for missed deadlines or misdiagnosis of an incident. We urge the legislation to include a safe harbor for small, covered entities operating in good faith.

**Conclusion**

We appreciate you raising the profile of a critical issue for the financial ecosystem, consumers, and the national economy.

Thank you again for the opportunity to testify today and to offer my perspective as a community banker and industry representative.

I look forward to your questions.

Written statement of proposed testimony by Carlos Vazquez for the Consumer Protection and Financial Institution subcommittee hearing on Cyber Threats, Consumer Data, and the Financial System

**Evolving cybersecurity threats:**

Cybersecurity is and always will be in a state of change. Yesterday the threat was malware, viruses and malicious executables inserted into a company's network. Today, ransomware, social engineering and supply chain attacks are the threats of the day. Tomorrow will see more of the same, plus deep fake technology, quantum processing (which may allow for easy compromise of all current cypher technology), and yet-unknown vulnerabilities in current hardware and software deployed by security departments in all companies.

Security departments are tasked with ensuring their data is and remains Confidential, with Integrity and Available (CIA) for those that require access to the data. The cost to ensure the CIA of data is tremendous and will continue to grow as technology evolves to counter the threat of APT groups and the day-to-day hackers trying to gain access to our networks and data for financial gain.

All financial institutions, especially credit unions with limited technical skills and funding, will need to ensure their strategies, for the current year to 3 to 5 years out, will be adaptable to meet the constant change in the threat landscape that affects cybersecurity.

**Consumer data protection challenges:**

People, processes, and technology are the challenges credit unions face to ensure our members' data is protected from malicious actors. Statistics show that in the financial services industry, a massive shortage exists in skilled security professionals which are required to manage the sophisticated tools in use today. Technology will constantly be changing and improving to counter the threat landscape brought to us by the malicious actors bent on breaking into our networks, via whatever means available, to steal our data for their own financial gain. The technology will not get cheaper; thus, it will be a challenge for the smaller institutions to both acquire and maintain it.

Training of employees is a challenge as social engineering has become the cheapest method of late for the malicious actors to trick users into providing credentials required to access the networks. Constant training is not only an escalating cost but a challenge to implement because employees either become weary or immune to the visual reminders of cyber hygiene.

Regulatory requirements can also present a challenge to financial institutions, especially smaller credit unions. Many may not have the ability or finances to maintain dedicated departments to ensure regulations are understood and met. For those financial institutions who need to meet regulations such as GDPR, the cost will be enormous in how to manage individual requests for management of their personal data.

Vendor management is another challenge facing financial institutions. With the supply chain breaches of 2021, it has highlighted the need to redo contracts with vendors to ensure transparency of any breach affecting the vendor. Many financial institutions will assume they are transferring their risk to

their vendors when they provide their data to those vendors. Although the risk may be transferred to the vendor ultimately the risk stays with the financial institution as our members expect us to secure their data. Vendors must have the same regulatory requirements to ensure data remains secure as the financial institutions themselves.

With the constant news of a new breach or ransomware affecting third-party vendors it becomes imperative that vendors do not become relaxed in securing our members' data. Vendors could easily have a runbook that assumes a breach can be fixed by social media messages and the hope their breach is only today's news cycle and quickly forgotten. Our members financial well-being is not trivial to us and should not be trivial to the vendors that have access to the data entrusted to us by our members.

**Effort by government agencies to Strengthen cybersecurity defenses:**

Data sharing (breaches, new vulnerabilities / patching, Advance Persistent Threat (APT) information) is paramount in ensuring all financial institution security departments are up to date on all threats affecting their security landscape. CISA, Homeland Security and Financial Services Information Sharing and Analysis Center (FS-ISAC) all are doing a great job in disseminating said information in a timely manner. It does fall on the financial institutions to ensure they are part of the data sharing network.

Webinars, conferences, and summits all provide the same information sharing that is very important in staying current with the threat landscape. In several recent summits there was participation by CISA and Homeland Security as guest speakers or presenters. Having these agencies present at these gatherings is very helpful and important as the discussions presented provide either information needed or some form of reassurance that the government is standing with financial institutions in their battle against the malicious actors.

**Strengths and weaknesses of the current legal framework governing data security and privacy in the financial sector**

The National Credit Union Administration (NCUA) is seeking legislative authority to have oversight over Credit Union Service Organizations (CUSOs) and third-party vendors that offer services to credit unions. The NCUA' Chairman sits on the Financial Stability Oversight Council (FSOC). The NCUA is the only federal agency that currently does not have this statutory authority as it relates to vendors that serve banking organizations. We believe credit unions deserve a regulator with parity in this regard.

Canvas Credit Union (located in Colorado) is supportive of parity for NCUA with the other federal regulators if the NCUA shares its information with state Regulators. Further, as vendors move offshore or go public it becomes increasingly challenging to hold some critical vendors accountable when we expect information from them.

*Statement for the Record*

*On Behalf of the*

**American Bankers Association**

*Before the*

**Consumer Protection and Financial Institutions Subcommittee**

*Of the*

**House Financial Services Committee**

**November 3, 2021**


Statement for the Record

*On Behalf of the*

**American Bankers Association**

*Before the*

**Consumer Protection and Financial Institutions Subcommittee**

*Of the*

**House Financial Services Committee**

**November 3, 2021**

Chairman Perlmutter and Ranking Member Luetkemeyer, thank you for the opportunity to submit this statement for the record on behalf of the members of the American Bankers Association (ABA)[1] for the hearing titled "Cyber Threats, Consumer Data, and the Financial System."

Banks are already subject to a wide-range of data protection, privacy and cybersecurity laws and regulations, and for many years have devoted the time, energy, and resources necessary to secure and protect data and earn the trust of our customers. ABA members are working hard to ensure that consumers remain protected from cyber-attacks, data breaches and other threats that put their sensitive personal and financial data at risk. These threats are constantly evolving and as consumers access a wide range and often novel financial services offerings, it is critical to ensure they retain the protections they have come to expect from their bank. Our statement summarizes current regulatory requirements that protect consumer data and privacy, our views on cybersecurity, and other threats to consumer data and makes several policy recommendations for Congressional and regulatory action to ensure that this data is protected going forward.

[1] The American Bankers Association is the voice of the nation's $22.8 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard nearly $19 trillion in deposits and extend $11 trillion in loans. Learn more at www.aba.com.

**Overview**

- GLBA and Data Privacy Protection. Banks are already subject to several data privacy laws and regulations, including Title V of the Gramm-Leach Bliley Act (GLBA). Any new legislation focusing on data privacy should take into consideration existing laws that apply to financial institutions and avoid new requirements that duplicate or are inconsistent with those laws, and should also preempt the existing patch-work of state data privacy laws.

- Cybersecurity. Our sector has devoted substantial time, energy, and resources to protecting our systems and consumer data. Cyber-enabled fraud and ransomware attacks are on the rise. Several bills have been introduced in the House and Senate requiring private sector entities to report significant cyber-attacks and ransomware payments to the Department of Homeland Security (DHS). Reporting such incidents is not enough, Congress should also ensure that the federal government and DHS effectively share threat information with the private sector on a timely basis and provide tools to help private entities mitigate the effects of the attacks and prevent future attacks.

- Data Aggregators. Consumer data is playing an ever-increasing role in all aspects of our economy. Section 1033 of the Dodd-Frank Act (DFA) guarantees consumers the right to access their financial data. Non-bank data aggregators hold a tremendous amount of consumer data. The Consumer Financial Protection Bureau (CFPB) has Section 1033 on its rulemaking agenda for 2022. Congress should urge the CFPB to bring non-bank data aggregators under its direct supervision.

- Payments. The financial marketplace has become a hotbed of innovation with new products and services being offered to consumers at an ever- accelerating pace. Monoline fintech firms, nonbank payment providers, large technology firms and decentralized finance technologies like cryptocurrency have entered the market and some are seeking access to the payments system, while seeking to avoid the full bank regulatory framework including data privacy and consumer protections. There should be

a high-bar for access to the payments system. Congress, the Federal Reserve Board, and other policy-makers should ensure that the stringent rules that apply to banks should be applied to any entity that offers bank-like products or services.

## A. Banks and Financial Institutions Are Subject to Extensive Data Protection and Privacy Laws

Banks believe strongly in protecting consumers' sensitive personal and financial information and their privacy. For hundreds of years, customers have relied on banks to protect the privacy of their financial information. Because banks are literally at the center of people's financial lives, our industry has long been subject to federal and state data protection and privacy laws. For example, Title V of the Gramm-Leach-Bliley Act (GLBA) not only requires banks to protect the security and confidentiality of customer records and information, but it also requires banks to provide consumers with notice of their privacy practices and limits the disclosure of financial and other consumer information with nonaffiliated third parties.

In enacting the GLBA in 1999, Congress stressed how critical privacy and data security is within the financial industry.[2] In this regard, it was Congress' intent that a financial institution's privacy practices must be readily accessible and easy to understand ("transparent") so that consumers can make well-informed choices. For example, the GLBA requires banks to provide notice to their customers about their information collection policies and practices. The notice is required to be clear and conspicuous and accurately describe the consumer's right to opt-out of the sharing of personal information with non-affiliated third parties if the bank shares customer information with such parties outside of exceptions.

Most banks make their GLBA privacy notices easily accessible on their websites. In this regard, many banks provide these disclosures using a standardized model template issued by the Consumer Financial Protection Bureau (CFPB) that is designed to follow the same format used

[2] *See* 15 U.S.C. § 6801(a) (stating that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information").

for nutrition labeling on food products. The current disclosures for consumers were developed over years of effort by federal regulators and the industry. Similar transparency about data collection and information sharing that is provided by the financial sector should be available to consumers no matter the type of company with whom they do business. For purposes of Federal privacy legislation, the GLBA should be considered a tried-and-true model for transparency.

In addition to transparency, the GLBA generally prohibits a bank from providing customer information to a nonaffiliated third party unless the bank has provided the customer with notice and an opportunity to opt out and the customer has not elected to opt out of such sharing. In this regard, the GLBA contains carefully crafted exceptions to the limitations on disclosures to nonaffiliated third parties that are designed to ensure that financial markets, products, and services that depend on the flow of financial information function efficiently for the benefit of the consumer, the financial institution, and the financial markets generally. For example, the GLBA permits a bank to disclose customer information to a nonaffiliated third party "as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes" or in connection with "[s]ervicing or processing a financial product or service that a consumer requests or authorizes" or "[m]aintaining or servicing the consumer's account with" the bank. The exceptions are also designed to ensure that banks can comply with other legal and regulatory mandates and be able to share information to prevent fraud and illicit finance. Notwithstanding these exceptions, the GLBA generally prohibits a bank from disclosing a customer's account number or similar form of access number or access code for a consumer's credit card account, deposit account, share account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through e-mail.

The GLBA also required the federal regulatory agencies to establish standards for safeguarding customer information. These standards require financial institutions to ensure the security and confidentiality of customer information, protect against any anticipated threats to such information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. And, since April 1, 2005, the federal banking agencies have required banks to have in place incident response programs to address security incidents involving unauthorized access to customer information, including notifying customers of possible breaches when appropriate.

Banks also are subject to other, decades-old federal financial privacy and data protection laws, including the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA). The FCRA, among other things, restricts the collection, use and sharing of information that is used to determine a consumer's eligibility for, among other things, credit, insurance, or employment. The FCRA functions to limit the extent to which affiliated financial institutions may share with each other information relating to consumers, including requiring notice and an opportunity to opt out before sharing non-transaction or non-experience information (*e.g.*, application information) that is used to determine eligibility for credit. Even to the extent that the FCRA permits affiliated financial institutions to share consumer information (*e.g.*, pursuant to notice and an opportunity to opt out), the FCRA limits the use of certain information for marketing if the information is received from an affiliate, including requiring notice and an opportunity to opt out before using the information for marketing purposes.

The RFPA protects individuals against unwarranted searches of personal financial records by the federal government. For example, a bank may not provide a federal government entity with access to copies of or the information contained in a customer's financial records except as permitted by the RFPA (*e.g.*, in response to a search warrant). Most states have similar laws limiting the disclosure of financial records to state government entities.

In addition, depending on their specific activities, a bank may be subject to a host of other federal privacy laws, including the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the CAN-SPAM Act, the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, and the Driver's Privacy Protection Act, among others.

Banks are also subject to strict regulatory oversight and regular exams regarding their compliance with data protection and privacy laws. This oversight includes the Federal Financial Institutions Examination Council Information Technology Examination Handbook, which is an extensive document with over 1,000 pages of IT guidance and examination instructions used by banking regulators to measure compliance with IT governance and information security program management.

**B. Data Privacy Legislation**

Congress has long recognized the importance of privacy for financial institutions and put into place a regulatory framework of strong privacy protections balanced with commonsense exceptions to minimize marketplace disruptions while maintaining a high level of consumer safeguards. These protections have been buttressed by a number of other laws with strong privacy protections, and banks and their federal and state regulators work aggressively to ensure consumers remain strongly protected.

We believe that Title V of the GLBA played a critical role in the development of privacy legislation in this country. The GLBA represented this country's first effort to regulate the privacy practices of a specific sector and should be recognized as an important benchmark. Moreover, the GLBA contributed to ensuing development of other sector-specific federal laws (e.g., HIPAA) and broader state data protection laws, particularly breach notification and data security.

Given the passage of time and even recent state efforts to adopt generally applicable privacy legislation, it is fair to at least question whether the GLBA should be updated. It is noteworthy that each of the new state privacy laws (*e.g.*, California, Colorado, and Virginia) includes an exception for entities covered by the GLBA.[3] However, if Congress considers a "refresh" of the GLBA, it is critical to consider the potential unintended consequences to the financial system, accounts, and transactions. This is what Congress did in 1999 by ensuring that well-crafted exceptions were in place to allow financial institutions to disclose customer information in order to process transactions and to fight fraud. In new data privacy legislation, Congress should carefully consider whether any specific privacy right (beyond those already included in the GLBA) are appropriate with respect to the types of information that financial institutions maintain about consumer financial accounts. For example, while the "right to be forgotten" may make sense with respect to a consumer's social media accounts or other online profiles, it should not be applied with respect to data surrounding a consumer's financial

[3] Colorado and Virginia explicitly chose to provide a complete GLBA exception, while even CA recognized the importance of the exemption for information covered by GLBA.

accounts. It would not make sense to allow customers to "delete" mortgage loan or credit card information.

While it is critical that any new Federal privacy law take into consideration existing privacy laws, such as the GLBA, that apply to financial institutions and avoid provisions that duplicate or are inconsistent with those laws. It should also preempt the existing patchwork of state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system. Having a single federal standard would ensure that consumers receive the same privacy rights and protections regardless of where they may live. A variety of state laws not only makes compliance challenging for financial institutions, but makes it very difficult for consumers to understand – and protect – their own privacy rights; the greater the variation in state laws, the greater confusion and conflict between states and the less transparent the entire regime becomes.

## C. **Cyber Attacks, Data Aggregation and Other Threats to Data Security**

Cybersecurity Threats

There are several ongoing trends with the potential to significantly increase risk to the U.S. financial services industry. Cyber-enabled fraud has become a preferred method used by organized crime and is evidenced by the rise in ransomware attacks. FinCEN recently released their financial trend analysis focused on ransomware and stated, "If current trends continue, SARs filed in 2021 are projected to have a higher ransomware-related transaction value than SARs filed in the previous 10 years combined."[4] This rising level of activity, coupled with the difficulty of finding and successfully prosecuting the perpetrators, is certain to result in a continual increase in attacks.

Recently introduced legislative proposals focusing on ransomware and attacks on critical infrastructure center on increased reporting of incidents to various entities such as the

[4] Financial Trend Analysis - Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, page 3, FinCEN.

Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). While there is value in understanding the scope and scale of attacks, such reporting may not necessarily help any of the victims of these attacks. This is especially true if they create significant and unwelcome burdens, such as trying to meet overly narrow reporting windows while simultaneously trying to manage the impact of an attack. Additionally, some of these proposals do not account for the maturity and reporting requirements already in place in the financial sector. As stated earlier, GLBA has significant reporting requirements already in place for data breaches and the prudential regulators have implemented additional regulations around reporting breaches and cyber-attacks. Legislation focused on reporting cyber-attacks and ransomware should not create redundant reporting requirements for the financial sector. It should also not just focus on reporting but should include strong provisions requiring the federal government and DHS to make effective use of these reports to share threat information with private sector entities in a timely fashion and provide tools that would allow the private sector to respond, mitigate the attacks, and prevent ongoing and future attacks.

Data Aggregation

Data is playing an ever-increasing role in all aspects of our economy, and banking is no different. Today, both banks and fintechs companies offer products that rely on access to a consumer's financial data, which may be housed at another institution. These products range from budgeting tools to income verification for underwriting.

Section 1033 of Dodd Frank guarantees consumers the right to access their financial records in a standardized electronic format. This has been widely interpreted to extend to their ability to share this data with authorized third parties. In 2017 the CFPB began exploring this issue and ultimately issued a set of principles[5] that outline how consumers should be treated when they share their financial data. Since the principles were released, industry collaboration has led to the development of technical standards, industry utilities, and other technologies and practices that can help enable responsible sharing within a safe and secure framework.

[5] See, https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/

The CFPB has refocused on this and issued an ANPR in 2021[6]. A recent Executive Order[7] has also highlighted 1033 as a priority. The CFPB currently has 1033 on its rulemaking agenda for Spring 2022. Banks support their customers' ability to access and share their financial data in a secure, transparent manner that gives them control. Consumer financial data is extremely sensitive and must be protected appropriately. As noted above, Congress has recognized the sensitivity of financial information and has provided protections for it under the GLBA, which creates a legal framework for protecting consumer data, and for sharing that data with third parties. However, when data leaves the secure bank ecosystem it is not always afforded these protections.

Traditionally, financial data was shared by a process known as "screen scraping," where a user would forfeit their login credentials creating risks and leaving consumers exposed. Banks, data aggregators, and other technology companies have worked together to invest in more secure API-based standards that give consumers transparency and control when they share their financial data. While we believe that continued industry collaboration is the best way to accomplish our shared goal, there are several regulatory clarifications and other recommendations that would help facilitate the continued development of a responsible data sharing ecosystem.[8]

As the CFPB considers next steps to encourage the development of a data ecosystem that protects consumers, we recommend that the Bureau continue supporting market developments that are already well underway. Overly prescriptive standards risk undermining the progress that has been made and if not well crafted, may leave consumers exposed. It could also stifle innovation that would potentially lead to secure approaches.

In addition, Congress should urge the CFPB to bring data aggregators under direct supervision. By the nature of their business, data aggregators hold a tremendous amount of consumer financial data. It is estimated that data aggregators hold the consumer log-in credentials for tens of millions of customers. Despite this, many consumers don't know that these

[6] See, https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/

[7] See, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/

[8] For a more detailed discussion of ABA's recommendations, see ABA Statement for the Record for the hearing titled "Preserving the Right of Consumers to Access Personal Financial Data" (Sept. 21, 2021) https://www.aba.com/advocacy/policy-analysis/aba-statement-for-the-record-preserving-the-right-of-consumers-to-access-personal-financial-data

intermediaries exist or how much of their information is being collected and shared. Consumers also are likely unaware of the potential risks to their information when it is shared. In most cases consumers do not have a direct relationship with these companies and must trust that their data are being handled appropriately. Proactive supervision is critical to identifying risks before any harm is done to consumers.

A cornerstone of Title X of the Dodd-Frank Act was the authority given to the CFPB to establish a supervisory program for nonbanks to ensure that federal consumer financial law is "enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition." Experience demonstrates that consumer protection laws and regulations must be enforced in a fair and comparable way if there is to be any hope that the legal and regulatory obligations are observed. ABA believes that establishing accountability across all providers of comparable financial products and services is a fundamental mission of the CFPB. This is especially important for data aggregators, given the sensitive consumer financial information they store and process.

The bulk of the data processing in this area is managed by a select group of large companies. Accordingly, the CFPB should expeditiously initiate the rulemaking process under Dodd-Frank Act 1024 to define those "larger participants" in the market for consumer financial data that will be subject to regular reporting and examination by the CFPB. Once the CFPB has imposed supervisory authority over the larger data aggregators, it will be better able to monitor – and react to – risks to consumers in this rapidly evolving marketplace.

Congress should also urge the CFPB to coordinate with banking regulators in any rulemaking because implementation of Section 1033 has wide-reaching implications for banks. Because of the sensitive nature of financial data, there are serious safety and soundness concerns that must be addressed. This is why Section 1033 requires the CFPB to "consult with the Federal banking agencies and the Federal Trade Commission," when prescribing any rules.

Third-Party Risk - NCUA Vendor Authority

Congress should take a serious look at the interplay between Credit Union Service Organizations (CUSOs) and the safety-and-soundness risks to the broader credit union system and to the protection of consumer data and privacy. CUSOs are vendors designed to support

credit unions, including in cybersecurity, consumer data protection and other activities. NCUA has no supervisory authority over CUSOs, notwithstanding repeated calls from NCUA Board Members of both political parties as well as the agency's Inspector General.

This regulatory blind spot is more significant now than ever before. In October, over strenuous objections from NCUA's Chairman, the agency finalized a proposal allowing CUSOs to engage in all forms of lending, including auto lending and payday lending. Because of the absence of vendor authority, NCUA has no authority to supervise or examine CUSOs for compliance with federal laws, including data protection, privacy federal consumer financial protection laws, creating what NCUA's Chairman termed a "wild west" of regulation and putting consumers at risk.

It is very troubling that the NCUA has authorized extensive CUSO activities without ensuring that consumers are protected from potential misuse and abuse of those activities. The new CUSO rule will also dilute the common bond requirement, since CUSOs need not serve credit union members, thereby moving credit unions even further adrift from their core mission to their membership. This raises significant competitive and reputation risks for credit unions, and more broadly, for markets and the financial services industry. We encourage the Committee to closely examine this rule and its potential consequences.

D. Access to the Payments System

Today, banks face a range of competitors and disruptors in the financial marketplace, including monoline fintech firms, nonbank payment providers and decentralized finance technologies like cryptocurrency and large technology firms. Only banks, however, offer the full financial services "bundle" of insured deposits that fund consumer and commercial loans, paired with access to the payments system. With this product bundle comes a robust set of data privacy and consumer protections and regulatory supervision. Banks are subject to safety and soundness supervision, regulatory capital and liquidity requirements, consumer protection rules, and affirmative obligations to demonstrate their service to their local areas via the Community Reinvestment Act.

Many nonbank competitors have business models that rely on a kind of regulatory arbitrage in which they can offer one or several aspects of the banking bundle while avoiding the full banking regulatory framework. We see this clearly in the rise of payments charters or

"special purpose national bank charters" that would aim to provide payments system access to companies that—because they do not hold insured deposits or do not lend—would not be subject to the same regulations as banks.

There should be a high bar for access to the payments system. Twenty years ago, in the days after the 9/11 attacks, the country learned just how critical regulated institutions are to payments. At that time, check clearing—managed by the Federal Reserve Banks—involved checks being shipped across the country via overnight airmail delivery. With U.S. airspace closed for several days and checks unable to be processed, the Federal Reserve provided credit on checks on their usual availability schedule. This was only possible because the Federal Reserve supervised the parties participating in the check clearing system and knew they would have sufficient liquidity to cover the checks. Supervision and high standards built up trust, and this lesson should be applied today as the Federal Reserve considers what entities may access our modern digital payments system.

Most importantly, consumers trust banks and the products they provide. According to Morning Consult research commissioned by ABA, nearly half of Americans trust banks more than any other company to keep their data safe, compared to just 12 percent who said the same for nonbank payment providers. Fifty-six percent of Americans say they prefer to receive financial services from a bank versus just 17 percent who said they would prefer to bank with the financial services division of a technology company.[9]

Into the existing payment system, interest has turned to new digital currencies or cryptocurrencies. Cryptocurrencies like bitcoin were designed explicitly to disrupt the banking business model and disintermediate them—allowing for "trustless" finance. Ironically, consumers trust banks *so much* that when they want to access crypto, they would rather do so through their banks. The fintech firm NYDIG surveyed bitcoin holders and found that 81 percent of them would move their bitcoin to a bank if it offered secure storage.[10]

One reason consumers trust banks is that they know their personal data is secure. As noted above, while banks are subject to robust privacy and data security requirements through

[9] See, https://bankingjournal.aba.com/2021/10/morning-consult-poll-banks-get-top-approval-ratings-from-consumers/

[10] See, https://nydig.com/research/nydig-bitcoin-banking-survey

the GLBA and other privacy laws, we understand that some nonbank fintechs take the position that they are not subject to the same requirements. Moreover, some nonbank fintechs may not have the same incentive to protect customer data, and may be more interested in profiting from providing third parties with access to that data. In fact, access to consumer financial transaction data may be the very reason large tech companies are interested in the payments space. We believe that it is important that the CFPB take a more proactive approach in identifying nonbank fintechs that are "financial institutions" for purposes of, and subject to, the GLBA and ensuring that those entities comply with the relevant obligations and limitations imposed by the GLBA. Consumers should receive the same privacy and data security protections at any financial institution.

Congress, the Fed and other policy makers should ensure that the stringent rules for banks should be applied to others looking to offer bank-like services. In that regard, we agree with concerns expressed by CFPB Director Rohit Chopra in his October 28 testimony before the House Financial Services Committee and the Senate Banking Committee about the involvement of big tech companies in the payments system and that they should be subject to the same rules and regulations as local banks and other financial institutions when it comes to data privacy.[11]

**Conclusion**

Banks of all sizes remain at the center of consumers' and businesses' financial lives and to continue to provide the lifeblood of the U.S. economy. Our members are dedicated to the best possible cybersecurity and to protecting the sensitive data and privacy of consumers. Banks are already subject to a wide-range of data protection, privacy and cybersecurity laws and regulations, and for many years have devoted the time, energy, and resources necessary to secure and protect data and earn the trust of our customers. ABA members are working hard to ensure that consumers remain protected from cyber-attacks, data breaches and other threats that put their sensitive personal and financial data at risk. These threats are constantly evolving and as consumers access a wide range and often novel financial services offerings, it is critical to ensure

[11] See, https://www.consumerfinance.gov/about-us/newsroom/written-testimony-director-rohit-chopra-before-house-committee-financial-services/

they retain the protections they have come to expect from their bank. We support legislation and policy that closes regulatory gaps that put the financial system and consumers at risk.

Credit Union National Association
CUNA

Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

99 M Street SE
Suite 300
Washington, DC 20003-3799

November 3, 2021

The Honorable Ed Perlmutter
Chairman
Subcommittee on Consumer Protection and Financial Institutions
House Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Blaine Luetkemeyer
Ranking Member
Subcommittee on Consumer Protection and Financial Institutions
House Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Perlmutter and Ranking Member Luetkemeyer,

On behalf of America's credit unions, I am writing regarding the hearing entitled, "Cyber Threats, Consumer Data, and the Financial System." The Credit Union National Association (CUNA) represents America's credit unions and their more than 120 million members.

We appreciate the Committee bringing cyber and data security and privacy to the forefront. Credit unions strongly support the enactment of a national data security and data privacy law that includes robust security standards that apply to all who collect or hold personal data and is preemptive of state laws. We firmly believe that there can be no data privacy until there is strong data security. With that in mind, credit unions call on Congress to pass a robust national data security standard that would cover all entities that collect consumer information and hold those who jeopardize that data accountable through regulatory enforcement. Securing and protecting consumer data is important not only for their individual financial health but as a further safeguard against rogue international agents and interference by foreign governments.

Data privacy and data security are major concerns for Americans given the frequency of reports of misuse of personally identifiable information (PII) data by businesses and breaches by criminal actors, some of which are state sponsored. Since 2005, there have been more than 10,000 data breaches, exposing as nearly 12 billion consumer records. These breaches have cost credit unions, banks and the consumers they serve hundreds of millions of dollars, and they have compromised the consumers' privacy, jeopardizing their financial security.

Stringent information security and privacy practices have long been part of the financial services industries' business practices and are necessary as financial institutions are entrusted with consumers personal information. This responsibility is reflected in the strong information security and privacy laws that govern data practices for the financial services industry as set forth in the Gramm Leach Bliley Act ("GLBA"). GLBA's protection requirements are strengthened by federal and state regulators examinations compliance with the GLBA's requirements and robust enforcement for violations.

Although protecting members' data is of paramount importance to credit unions, credit unions and their members are adversely impacted by lax data security standards at other businesses. For example, CUNA members have reported a massive increase in fraud against state unemployment insurance programs. These

reports have been confirmed by the United States Secret Service. The fraud appears to be mainly coming from an international fraud ring that has the capacity to exploit many states' unemployment programs. According to the Secret Service, the criminals are likely in possession of a vast amount of PII, which they are using to apply for unemployment insurance. It is almost certain that this PII was stolen in a data breach or many data breaches and it is now being used to exploit state unemployment insurance programs. This is clearly and example of how the multiple data breaches where PII has been stolen are causing harm to Americans and costing everyone money.

With that in mind, credit unions call on the Committee and Congress to follow the principles outlined below for Federal privacy and data security legislation:

**New Privacy and Data Security Laws Should Keep GLBA Intact:** Congress should leave financial services' robust data and privacy requirements in place. Financial services and the healthcare industry are subject to federal data privacy laws. The GLBA and the Health Insurance Portability and Accountability Act (HIPAA) have protected American's PII for over two decades and should be left in place as financial services and healthcare and their respective regulators have developed regulations, guidance and procedures for compliance.

**Data Privacy and Data Security Are Hand in Glove:** Any new privacy law should include both data privacy and data security standards. Simply put, data cannot be kept private unless it is also secured. Congress should enact robust data security standards to accompany and support data privacy standards.

**Everyone Business Not Already Subject to Federal Law Should Follow the Same Rules:** The new law should cover all businesses, institutions and organizations. Consumers will lose if Congress focuses only on tech companies, credit-rating agencies, and other narrow sectors of the economy because any company that collects, uses or shares personal data or information can misuse the data or lose the data through breach.

**There Should Be One Rule for the Road:** Any new law should preempt state requirements to simplify compliance and create equal expectation and protection for all consumers. We understand that some states have strong security and privacy requirements. Congress should carefully examine those requirements and take the best approaches from state law, as appropriate. A patchwork of state laws with a federal standard as a floor will only perpetuate a security system littered with weak links. The federal law should be the ceiling and the ceiling should be high. Just like moving away from the sector specific approach, the goal should be to create a strong national standard for all to follow.

**Breach Disclosure and Consumer Notification Are Important, But These Requirements Alone Won't Enhance Security or Privacy:** Breach notification or disclosure requirements are important, but they are akin to sounding the alarm after the fire has burned down the building. By the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions, of individuals.

**Hold Entities that Jeopardize Consumer Privacy and Security Accountable Through Regulatory Enforcement:** The law should provide mechanisms to address the harms that result from privacy violations and security violations, including data breach. Increasingly, courts are recognizing rights of action for individuals and companies (including credit unions). However, individuals and companies should be afforded a private right of action to hold those that violate the law accountable, and regulators should have the ability to act against entities that violate the law.

**Recognize This Issue For What It Is – A National Security Issue:** More and more, data breaches that expose consumer PII are perpetrated by foreign governments and other rogue international entities. The proceeds from these attacks are being used to fund illicit activity. The nature of these breaches alone calls for a strong federal response that ensures all involved in collecting, holding and using PII do so with the security of the information of paramount concern. You simply cannot have data privacy unless there is data security.

On behalf of America's credit unions and their more than 120 million members, thank you for the opportunity to share our views.

Sincerely,

Jim Nussle
President & CEO

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

November 3, 2021

The Honorable Ed Perlmutter
Chairman, Subcommittee on Consumer Protection and Financial Institutions
Committee on Financial Services
House of Representatives
Washington, DC 20515

The Honorable Blaine Luetkemeyer
Ranking Member, Subcommittee on Consumer Protection and Financial Institutions
Committee on Financial Services
House of Representatives
Washington, DC 20515

Dear Chairman Perlmutter and Ranking Member Luetkemeyer:

On behalf of the members of the Electronic Transactions Association (ETA), we appreciate the opportunity to submit this statement for the record before the Subcommittee's hearing, "Cyber Threats, Consumer Data, and the Financial System."

The Electronic Transactions Association (ETA) is the world's leading advocacy and trade association for the payments industry. Our members span the breadth of significant payments and fintech companies, from the largest incumbent players to the emerging disruptors in the U.S and in more than a dozen countries around the world. ETA members make commerce possible by processing approximately $22.5 trillion annually in purchases worldwide and deploying payments innovation to merchants and consumers.

ETA and its members are dedicated to working with federal and state regulators to address the important and growing issue of cybersecurity. The prevailing cybersecurity best practices developed and implemented in the financial and payments industries are the product of innovation and cooperation between industry and government. ETA strongly encourages policymakers to be sensitive to the risk of applying a prescriptive regulatory framework that undermine the federal and self-regulatory efforts that have made in combatting cybersecurity threats in the financial industry.

To the extent additional cybersecurity requirements are necessary, ETA supports an industry-led and principles-based framework that promotes innovation and competition among all industry participants in the financial data marketplace that provides industry with flexibility to keep pace with innovation in cybersecurity technology and emerging cyber threats.

**ETA Supports a Flexible Uniform National Standard for Cybersecurity**
ETA believes that a flexible uniform national framework is the most effective approach for addressing cybersecurity risks. In the electronic transactions industry, financial information data is governed by federal law, including the Gramm-Leach-Bliley Act (GLBA), the Federal Trade Commission's Safeguards Rule, and robust self-regulatory programs, including the Payment Card Industry Data Security Standard (PCI-DSS), which sets forth requirements designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data.

Since taking effect in 2003, for example, the information security requirements imposed by the Safeguards Rule have been held up as a model set of elements for developing an information

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

security program. These elements have served as a foundation upon which financial institutions and services companies have built leading cybersecurity programs, leveraging the inherent flexibility of the Safeguards Rule to tailor information security practices and protocols that meet their unique business models, data use practices, and network environments.

The existing framework of state laws undermines the effectiveness of a federal and self-regulatory framework. The development of separate state regimes not only increases the compliance burden of regulated entities, but also will undermine federal efforts to develop additional national best practices and standards for cybersecurity. If states continue to develop their own cybersecurity regimes, the focus of cybersecurity in the private sector will shift from developing new and innovative best practices to managing and complying with overlapping, or worse, conflicting, state and federal requirements.

For example, in January 2021, the prudential financial regulators proposed a rule relating to computer-security incident notification requirements for banking organizations and their bank service providers.[1] Additionally, Incident Reporting legislation pending in Congress, and when harmonized with the requirements of Section 2 of President *Biden's Executive Order on Improving the Nation's Cybersecurity*[2], have the potential to improve the nation's cybersecurity posture if appropriately developed and implemented. These efforts to streamline reporting requirements would ensure resources are used to combat malicious cyber threat activity, rather than customizing reports for various states.

We appreciate the opportunity to submit this letter for the record and the Subcommittee's leadership on this topic. If you have any questions, please contact me or ETA's Senior Vice President of Government Affairs, Scott Talbott, at stalbott@electran.org.

Sincerely,

Jeff Patchen
Senior Manager of Government Affairs
Electronic Transactions Association

[1] https://www.regulations.gov/document/OCC-2020-0038-0001
[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

**National Association of Federally-Insured Credit Unions**

November 2, 2021

The Honorable Ed Perlmutter
Chairman
Subcommittee on Consumer Protection and Financial Institutions
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

The Honorable Blaine Luetkemeyer
Ranking Member
Subcommittee on Consumer Protection and Financial Institutions
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

**Re: Tomorrow's Hearing on "Cyber Threats, Consumer Data, and the Financial System"**

Dear Chairman Perlmutter and Ranking Member Luetkemeyer:

I am writing on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) to share our thoughts ahead of tomorrow's hearing, "Cyber Threats, Consumer Data, and the Financial System." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 127 million consumers with personal and small business financial service products. NAFCU thanks the Subcommittee for holding this important hearing, and we appreciate the opportunity to share the perspective of our credit unions.

**NAFCU's Privacy Concerns with Proposed IRS Reporting Requirements**

Any discussion on consumer privacy must start with NAFCU reiterating our strong opposition to the provision in the fiscal year 2022 (FY 2022) Budget Resolution that proposes a new reporting requirement on financial institutions for account inflow and outflow information of American taxpayers to the Internal Revenue Service (IRS) for accounts with over $10,000 in transactions annually. We strongly urge Congress to not include any language enacting this provision in the *Build Back Better Act* and are pleased to see it not included in the draft text released last week.

This provision would be an invasion of privacy into countless Americans' daily lives. Financial institutions already face a robust reporting regime for financial transactions, such as 1099s, Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs). At any threshold, requiring credit unions to report on gross inflows and outflows of accounts poses regulatory costs and challenges while threatening to reduce participation in financial services and invade the privacy of hundreds of millions. While we support efforts to increase taxpayer compliance, we do not believe adding untested reporting requirements to an already heavily regulated industry is the answer. Instead, we would encourage Congress and the Administration to seek better solutions for taxpayer compliance, such as increased funding and support for IRS improvements. We remain committed to working with you in that effort.

**NAFCU Opposes Granting NCUA Additional Authority Over Vendors**

NAFCU continues to remain opposed to the legislative proposal under consideration by the Subcommittee, the *Strengthening Cybersecurity for the Financial Sector Act*. NAFCU and our member credit unions believe that cybersecurity, including the security of vendors that credit unions do business with, is an important issue. However, we are opposed to granting additional authority to the National Credit Union Administration (NCUA) to examine third parties at this time. NAFCU believes in a strong NCUA, but we also believe that the NCUA should stay focused on where their expertise lies—regulating credit unions. Credit unions fund the NCUA budget. Implementing such new authority for the NCUA would require significant expenditures by the agency. The history of the NCUA's budget growth has shown that these costs would ultimately be borne by credit unions and their members.

There are other tools already in place for the agency to get access to information about vendors. We believe the agency's time and resources are better focused on reducing regulatory burden by coordinating efforts among the financial regulators. The NCUA sits on the Federal Financial Institutions Examination Council (FFIEC) with the Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and the Federal Reserve. The FFIEC was created to coordinate examination findings and approach in the name of consistency and to avoid duplication. This means that as a member of the FFIEC, the NCUA should be able to request the results of an examination of a core processor from the other regulators and not have to send another exam team from the NCUA into their business and duplicate an examination. This would seem to be an unnecessary burden on these small businesses. Additionally, if the NCUA did its own examination, the likelihood of finding anything the other regulators did not would seem to be close to nil.

Instead of granting the NCUA vendor examination authority, Congress should encourage the agency to use the FFIEC and gain access to the information on exam findings on companies that have already been examined by other regulators. This would address the NCUA's concerns without creating additional costs to credit unions and increasing regulatory burdens on credit unions and small businesses.

**NAFCU Supports a National Data Security Standard**

As NAFCU has previously communicated to Congress, there is an urgent need for a national data security standard for entities that collect and store consumers' personal and financial information that are not already subject to the same stringent requirements as depository institutions. Unfortunately, retailers and fintechs are not held to the same data security expectations as depository institutions, which have faced rigorous cybersecurity exams for years under the *Gramm-Leach-Bliley Act* (GLBA). Far too often these companies are the targets of data thieves because they do not have the same standards in place as financial institutions. Credit unions suffer steep losses in re-establishing member safety after a data breach and are often forced to absorb fraud-related losses in its wake. Credit unions and their members are the victims in such a breach, as members turn to their credit union for answers and support when such breaches occur. As credit unions are not-for-profit cooperatives, credit union members are the ones that are ultimately impacted by these costs.

NAFCU believes that negligent entities should be held financially liable for any losses that occurred due to breaches on their end so that consumers are not left holding the bag. When a breach occurs, depository institutions should be made aware of the breach as soon as practicable so they can proactively monitor affected accounts. Finally, any new rules or regulations to implement these recommendations should recognize credit unions' compliance with GLBA and not place any new burdens on them.

As we have shared with you before, we recognize that a legislative solution to data security is a complex issue, and thus have established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to enact legislation to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other depository institutions are required to meet certain criteria for safekeeping consumers' personal information and are held accountable if those criteria are not met through examination and penalties. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers other entities who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on depository institutions under the GLBA.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by those who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the negligent entity who incurred the breach.

**NAFCU's Principles for a Federal Data Privacy Standard**

Entwined with data security is data privacy and the need to protect consumer information. In 2019, recognizing the importance of data privacy and the ongoing privacy debate, NAFCU issued a series of data privacy principles that call for a comprehensive federal data privacy standard that protects consumers, harmonizes existing federal data privacy laws, and preempts state privacy laws. As the Subcommittee works to achieve a path forward on federal data privacy legislation, NAFCU recommends you include the following elements as key aspects in any such bill:

- **A comprehensive national data security standard covering all entities that collect and store consumer information.** In order to protect consumers, retailers, fintech companies and any other organizations handling personal information should be required to provide reliable and secure information systems similar to those required of credit unions.

- **Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.** The patchwork of federal and state privacy laws creates an environment where consumers receive multiple disclosures on different information and their rights vary significantly across different types of organizations; this situation is confusing for consumers, burdensome for credit unions, and can only be resolved by a federal law that preempts state laws.

- **Delegation of enforcement authority to the appropriate sectoral regulator**. For credit unions, the NCUA should be the sole regulator. Allowing NCUA, which is well versed in the unique nature of credit unions and their operations, to continue to examine and enforce any privacy and cybersecurity requirements is the most efficient option for both credit unions and American taxpayers.

- **A safe harbor for businesses that take reasonable measures to comply with the privacy standards.** Any federal data privacy bill should provide for principles-based requirements based on an organization's specific operations and risk profile, and a safe harbor for organizations that design and implement appropriate measures.

- **Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.** Providing multiple privacy disclosures and opt-out mechanisms across multiple channels creates confusion for consumers and unreasonable burdens for credit unions. A new privacy law should incorporate the GLBA's requirements to avoid conflicting or duplicative disclosure requirements.

- **Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.** Actual damages to consumers are too difficult to establish by evidence and statutory damages for violations is incredibly ripe for frivolous lawsuits; sectoral regulators should have the power to assess scalable civil penalties, which can then be used to remedy and prevent consumer harm in a meaningful way.

**Regulation of Fintechs and Nonbanks**

As NAFCU testified before the Subcommittee in April 2021, the growth of fintech in recent years offers new opportunities for the delivery of financial services.[1] The use of financial technology can have a positive effect on credit union members. Credit unions have worked with fintech companies to improve efficiency in traditional banking, and many of the technologies that are commonplace today, such as credit cards and e-sign, would have once qualified as "fintech" when they were first introduced. Consumers today come to expect technological developments from their financial institution—from online banking to mobile bill pay. Many credit unions embrace innovations in technology to improve relationships with members and offer more convenient and faster access to financial products and services.

However, the growth of fintech can also present new threats and challenges as novel entities emerge in an underregulated environment. As such, NAFCU believes that Congress and regulators must ensure that when technology firms and fintechs compete with regulated financial institutions, they do so on a level playing field where smart regulations and consumer protections apply to all participants. NAFCU has outlined some of the challenges and opportunities in this area in a white paper which proposes regulatory recommendations for oversight of fintech companies.[2]

For example, fintech companies that specialize in lending, payments, or data aggregation present unique consumer protection concerns. A fintech company that permits consumers to consolidate control over multiple accounts on a single platform elevates the risk of fraud and may not be subject to regular cybersecurity examination and data privacy and protection requirements in the same way that credit unions are under the GLBA. Although non-bank lenders are subject to consumer protection rules, the connectivity and segregation of discrete services within the fintech marketplace can create supervisory challenges.

---

[1] House Committee on Financial Services Subcommittee on Consumer Protection and Financial Institutions, "Banking Innovation or Regulatory Evasion? Exploring Trends in Financial Institution Charters," April 15, 2021, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=407533.

[2] NAFCU, Regulatory Approaches to Financial Technology, available at https://www.nafcu.org/fintech-whitepaper.

Congress should ensure that the data security and privacy requirements for financial institutions in the GLBA, including supervision for compliance, apply to all who are handling consumer financial information and that programs for implementing these requirements conform to the guidance developed by FFIEC member agencies.

NAFCU also believes financial regulators have a role to play in the supervision and regulation of fintechs under their existing authorities. Congress should also be willing to step in and clarify the role of regulators when necessary. For example, NAFCU believes that the Consumer Financial Protection Bureau (CFPB) can play a role under its "larger participants" authority under the Dodd-Frank Act to regulate and supervise technology firms and fintech companies that enter into the financial services marketplace. If the CFPB does not believe it has this authority currently, Congress should examine granting the Bureau explicit authority in this area.

Congress should also consider creating an FFIEC subcommittee on emerging technology to monitor the risks posed by fintech companies and develop a joint approach for facilitating innovation. We would envision the subcommittee having the following under its charge:

a. To report its findings to Congress annually;
b. To define the parameters of responsible innovation to ensure consistent examination of emerging technologies;
c. To identify best practices for responsible innovation; and,
d. To recommend regulatory improvements to allow FFIEC-regulated institutions to adopt new technologies with greater legal certainty.

**Regulation of the Consumer Reporting Agencies (CRAs)**

High-profile data breaches in recent years have highlighted the need for addressing consumer data security issues at national credit bureaus and beyond. While credit bureaus, such as Equifax, are governed by data security standards set forth by the GLBA, they are not examined by a regulator for compliance with these standards in the same manner as depository institutions. For example, the 2017 Equifax breach reportedly occurred via a "known" security vulnerability that software companies had issued a patch to fix several weeks prior. If Equifax had acted to remedy the vulnerability in a reasonable period of time, this breach may not have occurred. Companies that knew or should have known about a threat and failed to take mitigating action must be held financially liable.

When a breach occurs at a credit bureau, depository institutions should be made aware of the breach as soon as practicable so they can proactively monitor affected accounts and limit the losses that in credit unions are ultimately borne by the members. Furthermore, compliance by credit bureaus with GLBA and these notification requirements should be examined for, and enforced by, a federal regulator. We do believe that there should be further examination as to whether the CFPB – as proposed by the *Enhancing Cybersecurity of Nationwide Consumer Reporting Agencies Act* before the Subcommittee – or the Federal Trade Commission (FTC) is the best approach to establishing appropriate standards in this area.

In conclusion, we appreciate the opportunity to share our input on this important topic and look forward to continuing to work with the Subcommittee on these issues. Should you have any questions or require any additional information, please contact me or Sarah Jacobs, NAFCU's Associate Director of Legislative Affairs, at sjacobs@nafcu.org.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Consumer Protection and Financial Institutions

November 3, 2021

The Honorable Ed Perlmutter
Chairman
Subcommittee on Consumer Protection
and Financial Institutions
Committee on Financial Services
U.S. House of Representatives

The Honorable Blaine Luetkemeyer
Ranking Member
Subcommittee on Consumer Protection
and Financial Institutions
Committee on Financial Services
U.S. House of Representatives

Dear Chairman Perlmutter and Ranking Member Luetkemeyer:

On behalf of SentiLink, I am pleased to submit this statement for the record for your hearing titled "Cyber Threats, Consumer Data, and the Financial System." SentiLink provides industry-leading solutions to prevent synthetic fraud, identity theft, and other emerging fraud vectors at the point of account origination.

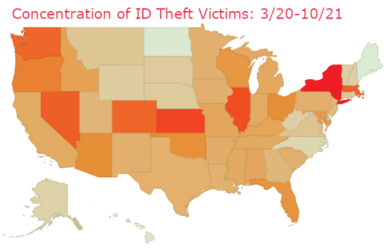
Cyber threats from nation-states and other well-organized actors are unquestionably a serious concern for policymakers and the financial services industry. As the Committee's hearing memo notes, attacks can take many forms -- from those designed to take down a financial institution's network and disrupt critical functions, to attacks targeted at individuals. These more localized, personal attacks all have a common theme: Compromising or manipulating identity data in order to commit fraud.

Of particular importance, I would like to highlight the increasing risk to the financial services industry from synthetic identity fraud (SIF). This type of fraud occurs when a criminal engineers a fake person using a fictitious name, date-of-birth and Social Security number (SSN). When this fake identity is used to apply for a financial product, it leads to the creation of a credit report for the made-up identity. Over time, and after an amount of artificial "credit building," the synthetic identity is used to open new accounts for purposes of commiting bust-out fraud, laundering money, or other financial crimes.

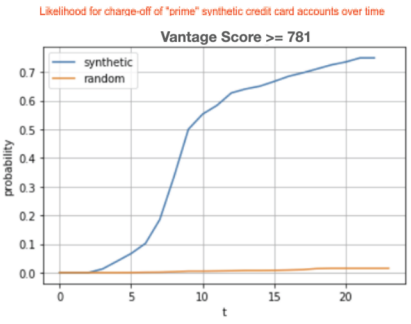
While SIF costs US lenders billions of dollars in losses annually, the financial industry isn't the only target. As the COVID pandemic revealed, governments at all levels can also be impacted by SIF. As we described in a previously submitted statement to the Committee, we have been able to identify synthetic identities, entirely fictitious businesses, and real businesses with fictitious employees that applied for various pandemic relief funds.

More broadly, identity crimes are a widespread problem that impacts the safety and soundness of the banking system, and financial health of US consumers. **We analyzed data from a sample of our financial institution partners and found that during the pandemic, a high concentration of**

**identity theft victims whose data was used to apply for accounts were located in New York, Illinois, Kansas, Colorado, Nevada and Washington (as illustrated by the darker colors on the accompanying map).** While criminals themselves and their associated fraud rings are still heavily concentrated in "hot spots" like Florida and California, our analysis demonstrates that victims are dispersed throughout the country.




For financial institutions, our analysis of the behavior of synthetic identities over time reveals the potential for increased financial losses. **Looking at the credit card market, for example, our data -- shown in the chart below -- illustrates how synthetic identities that have been built to a "prime"-level credit score tend to charge off 75% of the time within 23 months for an average loss of $13,000, compared to the performance of legitimate consumers who would be expected to charge off at a rate of 1.5% during the same time.** It is also important to recognize the impact on the broader financial system when identity and know-your-customer (KYC) safeguards are undermined by synthetic fraud.




Policymakers must ensure that robust identity verification requirements -- including for identity theft and synthetic identities -- are baked into the fundamentals of KYC rules and regulations. As we've observed, the risk to financial institutions of all sizes and charter types from identity fraud exists across the spectrum of financial products and services, including with basic checking account offerings.

We appreciate the opportunity to provide these comments and look forward to engaging with you and your colleagues to advance policy solutions that protect American consumers and businesses from identity crimes.

Sincerely,

Jason Kratovil
Head of Public Policy