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.