**Testimony on "Cybersecurity: Risks to Financial Services Industry and Its Preparedness"**
**By**
**Carl A. Kessler III**
**Senior Vice President & Chief Information Officer (CIO), First Mutual Holding Co.**

**Before the**
**Committee on Banking, Housing, and Urban Affairs**
**United States Senate**
**May 24, 2018**

Chairman Crapo, Ranking Member Brown and distinguished Members of the Committee, thank you for the opportunity to testify before you today. I am pleased that the Committee continues to place a focus on cybersecurity risks and their implications to the financial system, businesses, and consumers.

As Chief Information Officer of a holding company comprised of several mutual community banks, I will share the unique perspective of community banks on cybersecurity regulation, information sharing, community bank collaboration and customer transparency.

*Cybersecurity Regulation*

Two key regulatory changes have positively improved the approach of community banks in managing cybersecurity risks. In the wake of the Dodd Frank Act reforms, supervision of our affiliate banks migrated from the Office of Thrift Supervision (OTS) to the Office of the Comptroller of the Currency (OCC). The OCC has been consistent and adamant in raising all bank's readiness to address cybersecurity risks. Their outreach and guidance have yielded vast improvements in the cyber posture of community banks. In the last few years, the Federal Financial Institutions Examination Council (FFIEC) established the Cybersecurity Assessment Tool (CAT) for evaluating cyber controls in a uniform way among depository institutions.

Both regulatory actions have created a firm, but fair, supervisory approach in responding to emerging threats. While some may question these changes on the grounds of cost and a "one size fits all approach", it is indisputable that regulatory oversight protects both the banking system and the consumers. We have found that the regulators apply the FFIEC CAT tool in a manner consistent with the risk a bank poses. I believe that cybersecurity defenses and monitoring systems are integral infrastructure investments akin to those community banks have traditionally made in physical security safety. I encourage this Committee to continue its work with prudential regulators on these important matters.

With respect to OCC supervision and the advent of the FFIEC CAT, I understand both the perspectives of regional banks and community banks, having served in leadership capacities in both. I am pleased regulators use the same information technology (IT) examiners and general framework at institutions of all sizes. These examiners possess a strong understanding of cybersecurity risks and the controls deployed to protect banks and consumers. For any institution there is an inherent baseline of risk and a set of fundamental controls needed to protect consumer information. The approach of using dedicated IT examiners and practices fosters continuous improvement in preventing and detecting cybersecurity threats at institutions of all sizes.

At the same time, this approach also leads to ongoing dialogue with regulators. How much risk does our community bank present? What is most critical for the protection of our bank, our customers and our financial system? How should cybersecurity investment dollars be deployed? The FFIEC CAT helps institutions frame these risk questions. First, it provides a standard way to assess how much inherent risk an institution generates. Second, the FFIEC CAT provides guidelines for what controls might be appropriate to mitigate those risks.

After completing our holding company's assessment in 2015, we concluded that our existing information security program was well-aligned to the baseline expectations of the FFIEC CAT and, in fact, exceeded them. Subsequent actions focused our cybersecurity investment strategy to attain compliance with our level of risk and to address new threats as they arise.

Prudential regulation in conjunction with the FFIEC CAT is important to our bank's cyber readiness. Highly trained examiners are critical to administering the CAT. Because of the nature of the threat environment and the rapidly evolving domain of cybersecurity controls, an exam is never a static, check-the-box activity. It is always a dynamic conversation. My recommendation to this Committee is to ensure the consistent availability of highly-trained IT examiners whose skills are in high demand in both the public and private sectors.

Another consideration for the Committee is to ensure that similar cybersecurity rigor exists among non-bank financial services companies. How do we safeguard customer data at companies outside the oversight of prudential regulators?

*Information Sharing*

As the cyber threat landscape evolves, a critical enabler is timely access to information sharing of active threats with community banks, through public and private partnerships.

To address the Committee's question of "what more needs to be done by the private sector and government to help protect companies' and consumers' information", we must first identify where the significant risks lie. According to the Independent Community Bankers of America (ICBA), 99.5% of all banks are community institutions, half of which have assets under $250 million.[1] Almost all community banks do not operate an in-house transaction processing center. In other words, most community banks do not process customer transactions in their own data centers. They rely on a network of third party service providers to deliver banking services. While maintaining primary accountability for safeguarding consumers' information, we rely on third party providers including core processors, payments networks, and larger banks.

Only a few core processors provide IT services, such as customer transaction processing, mobile banking, and Bank Secrecy Act/Anti-money Laundering solutions. All banks interact through networks (ATM, debit card, and ACH) which are the backbone of the payments system. Some large banks provide processing for community banks through white labelled correspondent services. Although community banks represent the largest segment of banks in number, the risks associated with technology

[1] See ICBA Stats & Facts available at http://www.icba.org/go-local/why-go-local/stats-facts

operations are aggregated in the data centers of just a few core processors[2], payments networks and large banks.

Clearly, this concentration of IT services provides both advantages and challenges for managing community bank cybersecurity. The advantage is that through scale, the large service providers have more resources to address cyber threats. An additional benefit could also be realized if these providers acted transparently and shared cyber threat information with industry partnerships like the Financial Services Information Sharing and Analysis Center (FS-ISAC) and with their community bank clients.

Core processors are active acquirers of technology companies and continually roll out new products. Although a core processor's information security plan may be sound today, each new acquisition introduces its own risk[3] into the environment. Thus, risk is constantly shifting within a core provider, and by extension to community banks and consumers.

I know our core processor is reviewed regularly by the OCC and FFIEC. We have limited access to the results of these reviews. If a bank were in the center of a significant event like a contract renewal or if there were a security breach in the recent past, the bank can request additional information. Community banks also have access to third party audits conducted on a core processor's controls. Such a report is limited and only communicates if a core processor's controls are deemed effective. The actual number of breaches is typically not disclosed. Thus, a community bank must trust that if there is a significant pattern of breaches, its regulator will ensure that the causes are identified and remediated. The only way to know if a breach has occurred is if the bank is directly impacted or if the breach is significant enough to result in a news story that names a bank that happens to use that same service provider. Although these third parties are the stewards of our customer's information, we have very little insight into their overall security performance. In summary, law and regulation require banks to monitor closely the effectiveness of their service provider's controls related to cybersecurity and protecting non-public customer information. The current system relies on a high degree of blind trust in a service provider with limited transparency. This opaque approach runs contrary to best practices in information sharing and vendor management.

To partially compensate for this lack of transparency, banks I manage use a third party to track the information security performance of critical providers. My desire is more transparency in how service providers protect our customer information. For example, one solution might be to create a cybersecurity scorecard aggregating data from many sources including regulatory reviews. Such an approach must be carefully weighed against a chilling effect on information sharing. This scorecard, properly executed by a trusted third party, would enable banks to make better choices as they select vendors and create positive momentum toward control improvements.

It is important to explain what "information sharing" and "transparency" mean to a community bank. The key for banks is that a comprehensive ecosystem of financial services providers shares threat

---

[2] The top three core processors hold a 70% market-share although how much of that is conducted in their data center versus the banks' data centers is unclear. https://bankinnovation.net/2018/02/fiserv-has-largest-u-s-marketshare-of-top-bank-core-processors/

[3] In April, American Banker ran this story "BankThink Banks are from Mars, fintechs are from Venus: Bridging the matchmaking gap" by Terry Ammons which does a good job of representing the risks of a fintech acquisition; available at https://www.americanbanker.com/opinion/banks-are-from-mars-fintechs-are-from-venus-bridging-the-matchmaking-gap

information in real time to an entity qualified to analyze, verify, and communicate it immediately to a bank where it can be used to adapt its controls.

FS-ISAC pioneered this kind of service and our bank was an early adopter. Upon validation of a threat by FS-ISAC, critical information such as the internet address of the attacker was automatically sent to our firewalls and blocked. This solution required our bank to setup a duplicative connection. Our ideal solution involves a close partnership between banks, our third-party service providers, a trusted third party and our security provider so that threats flow immediately to us via the existing mechanisms we have in place. The goal is to respond in seconds or minutes rather than days or weeks.

The most critical factor in thwarting a cyberattack is speed. The technology continues to improve as machine learning and artificial intelligence become more prevalent. The technology though cannot act on data it does not have. Important questions remain regarding if, when and how businesses can share threat and/or breach information. In my conversations within the industry, there is still a great reluctance to share information. Liability, contract and privacy concerns are the most often cited reasons. I would suggest this is a good time to reexamine the effectiveness of cyber security law particularly as it affects information sharing. Timely information sharing is foundational to the industry's ability to combat a cyber threat. It may be worthwhile to require that service providers share threat and breach information with an authorized, trusted third party. In consideration for this sharing requirement, this Committee could consider expanding safe harbor liability provisions for third parties who meet certain strict requirements. This would clearly enhance consumer information protections.

*Community Bank Collaboration*

I would like to share a few unique and not-so-unique actions we have taken to help protect our customers. Established in 2015, our mutual holding company was founded on the belief that strong independent banks play a vital role in our communities. As Ohio's largest independent, depositor-owned entity, we are faced every day with the cost, complexity and capacity required to implement an effective information security program. We believe that our holding company model leverages these capabilities with our affiliate banks in a manner that they otherwise could not afford, design, or staff. In our three affiliations we have preserved a local banking presence, improved security controls and done so at a minimal marginal cost for the holding company. This proves the cost savings for individual small banks is a game changer. We believe this is a real, practical example of the kind of collaboration envisioned by the OCC in their January 2015 paper "An Opportunity for Community Banks: Working Together Collaboratively.[4]"

*Customer Transparency*

Finally, when talking about transparency and information sharing, we tend to focus on companies and government entities. In all instances however we need to put the consumer at the center of this discussion. We are encouraged by the ability of technology to empower our customers. For example, many of us receive real-time alerts regarding our debit cards or when our credit report changes. I know this hardly seems to address "what more needs to be done", but keep in mind it's

[4] https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/pub-other-community-banks-working-collaborately.PDF

always about improving the speed at which we can detect and react to a threat. Giving consumers the tools and access to information makes us all safer.

Transparency and information sharing with the consumer is paramount. A key challenge for banks is the complexity of customer notification and privacy laws that exist today. While clearly needed, the simplification and modernization of the relevant laws and regulations can enable information sharing and therefore enhance consumer protections. Certainly, any solution must guard against shifting the liability to consumers from those who failed to protect their data.

*Conclusion*

Key takeaways:

- Continue supporting the regulatory review process and the FFIEC CAT
- Encourage transparency regarding the effectiveness of the security programs of the third-party service providers in our financial system including non-bank entities
- Review the effectiveness of current cybersecurity law with a focus on information sharing
- Review how the existing complexity of customer information and privacy protections laws may be slowing down the exchange of critical threat information
- Encourage community banks to collaborate
- Engage and empower the customer as a valued part of the cybersecurity solution

The best way to protect consumers is to increase transparency and information sharing within the financial services cybersecurity ecosystem. This committee can help move this forward by encouraging the transparency of the performance of third party service providers. You can also help by passing legislation which further encourages information sharing so that active threats are identified and mitigated in minutes.

Thank you for the opportunity to testify before you today. I stand ready to work with you in any way that I can to protect consumers and our financial system and look forward to answering your questions.