Written Testimony of

Kenneth E. Bentsen, Jr., President and CEO, SIFMA

before the U.S. House of Representatives

Committee on Financial Services

Subcommittee on Financial Institutions and Consumer Credit

Hearing entitled "Data Security: Vulnerabilities and Opportunities for Improvement"

November 1, 2017

Chairman Luetkemeyer, Ranking Member Clay, and members of the Subcommittee, thank you for giving me the opportunity to testify today on the important topic of cybersecurity and data protection. The Securities Industry and Financial Markets Association (SIFMA)[1] represents hundreds of banks, broker-dealers, and asset managers who collectively are dedicated to protecting their systems and more importantly, their clients' data, from cyber-attacks. There is likely no greater threat to financial stability than a large-scale cyber event and so SIFMA and its member firms are deeply committed to improving our sector's cybersecurity resiliency and working with our government partners to protect the broader economy. Our members have invested tremendous monetary and human resources to develop and implement cyber defense and recovery mechanisms and we welcome the opportunity to discuss the progress made and challenges identified.

The cybersecurity landscape is complex with a wide array of hostile actors, including criminals seeking financial gain, nation states engaged in corporate espionage or worse, and terrorist groups seeking to disrupt markets and create fear. Cybercrime is now a bigger criminal enterprise than the global narcotics trade. The financial services industry is a top target facing tens of thousands of attacks each day. While data breaches of customer information dominate headlines, and are an appropriate concern for policymakers, a major cyberattack on critical financial market infrastructure or one that destroys records and financial data, is a risk with a potentially far larger impact on the economy.

While regulation and supervision of cyber preparedness has an important role in the collective cyber defense effort, the emergence of many regulations from multiple regulators may lead to a suboptimal balance of industry resources devoted to compliance versus security.

October marked National Cybersecurity Awareness Month, a prime opportunity for the industry and regulators alike to have assessed how cyber defense and response policies and protocols can be improved to protect our nation's critical infrastructure, including the financial markets. Enhanced harmonization of regulatory standards and supervision would improve the efficient use of critical

[1] SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over $2.5 trillion for businesses and municipalities in the U.S., serving clients with over $18.5 trillion in assets and managing more than $67 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

cyber resources. In simple terms: financial institutions shouldn't have to devote limited resources to redundant regulatory and supervisory requirements at the expense of actual security-based activities.

But it is important to recognize that no single actor – not the federal government, nor any individual firm – has the resources to protect markets from these threats on their own. It is critical that we establish a robust partnership between industry and government to mitigate cyber threats and their impact. The industry's resiliency will not be fully effective without the government's help, and vice versa.

Make no mistake, both the industry and our regulators are in complete agreement that cyber security and resiliency are and should be a top priority. And our collaboration with regulators on the matter has never been greater. Cybersecurity is truly a shared objective where the interests of the government and private sector are fully aligned. We are all targets and the industry remains vigilant to confront this risk every day.

For our part, the securities industry is constantly working to improve cyber defenses, resiliency and recovery through massive monetary investment in technology and personnel, regular training, industry exercises, and close coordination between the financial sector and the government, including our regulators. This is a C-Suite and Board-level issue and has been a top industry priority for several years. A strong collaboration between the government and private sector is key to success. Continued work to streamline and coordinate regulation would strengthen this partnership and help to better protect investors and the markets.

Today, I would like to outline some key areas of focus for SIFMA's members. While this list is not exhaustive of our cyber agenda, it may be timely and of interest to the Subcommittee. SIFMA's top priorities include: protecting customer data; coordinating cyber regulations across government; and ensuring that information shared with third-parties is adequately protected. I will also speak on SIFMA's efforts to prepare industry for cyber eventualities through industry-wide exercises that allow firms to simulate responding to attacks.

Data Protection

In recent years there have been an increasing number of highly visible data breaches, affecting billions of customer records. These breaches have targeted a broad range of organizations, from retailers and financial institutions to Federal and state governments and regulatory bodies. A recent study found that in the first half of this year, 918 data breaches resulted in a total of 1.9 billion records being accessed.[2] These attacks demonstrate that any public or private sector institution which holds sensitive information can, and indeed will be, a target of malicious actors. The development of sound practices by all members of the financial sector is critical. We have moved into a new era that requires us to be more tactical in our understanding of the data management lifecycle and what it might mean if that chain is broken by a malicious actor. All of us have a shared responsibility to protect sensitive information**.** Our members, clients and the public all expect our standards as a sector to be higher and our judgment to be sound.

Working with our members, along with our sister trade associations, SIFMA has recognized a number of best practices for the protection of sensitive data in the financial services sector. These practices draw on the experience of our member firms and their own policies and procedures, as well as industry standards such as the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity.[3]

The experiences of our members show the importance of developing a culture and practice dedicated to the protection of sensitive data including an investor's personal identifiable information or "PII." This requires focus across the entire ecosystem, extending from when the decision is first made to collect a given piece of data through its eventual destruction when no longer needed. At each of these stages, organizations must be committed to best practices to ensure that their systems and processes are protected.

Data protection begins with firms taking a risk-based look at what information they collect – do they have a business or regulatory purpose that requires them to hold this information? If sensitive

[2] https://blog.gemalto.com/security/2017/09/21/new-breach-level-index-findings-for-first-half-of-2017/
[3] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

information like social security numbers is not directly relevant and necessary, firms should refrain from collecting it.

Once firms have collected sensitive data, they should ensure that they have controls in place to protect it while it is being used or stored. This includes ensuring that access to sensitive data including investor information is restricted only to authorized users who need it to perform their jobs – and making sure that as individuals change their roles and responsibilities, their access to sensitive information is updated as well. Keeping access to this data focused only for those who need to use it helps reduce the potential points of risk. Firms should also have policies such as data loss prevention controls, multifactor authentication to control access to sensitive data, as well as maintain a detailed audit trail of how sensitive data is handled while in possession to identify any weaknesses or vulnerabilities.

In addition to protecting data within the four walls of their organization, firms should be mindful of the associated risks when they share sensitive information externally. Firms also need to understand the security controls in place at any organization they share sensitive information with, and ensure that the process of transferring information is secure, such as through encryption. Firms should also work to reduce risk by destroying sensitive data once it is no longer needed.

To further protect sensitive data, firms should also draw on the range of available information security, cybersecurity tools and expertise where appropriate – including vulnerability scans, penetration testing (e.g. manual ethical hacking, dynamic analysis), timely remediation of weaknesses once they are identified, robust security training for their teams, and procedures for notification of breaches.

This focus on data protection also extends beyond securities firms themselves to encompass other entities with whom we share information. The risks posed by third parties have been recognized by regulators in the U.S. and internationally, such as the Office of the Comptroller of the Currency (OCC)'s release on Third-Party Relationships: Risk Management Guidance.[4] To understand and mitigate these risk, firms have extensive vendor management and third-party risk assessment

[4] https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

programs. To help firms better understand the security environment at their third parties, SIFMA worked with the AICPA to help develop audit-based cyber attestations, based on NIST and other industry standards. As a highly-regulated sector, our members provide a tremendous range of sensitive information, including that of their retail and corporate clients, with regulators in accord with their supervisory mandates. This data is subject to protection and standards shaped by the Federal Information Security Modernization Act (FISMA), and given the ever-increasing risk, our sector is engaged in important dialogue with our government partners to ensure and enhance protections across the board.

Financial firms and regulatory agencies share a common goal in securing and protecting the data entrusted to them by clients and financial institutions. This information can include both personally identifiable information such as social security numbers, dates of birth, or other information provided by retail clients, as well as corporate data and intellectual property which institutional clients entrust to the financial services industry.

Consolidated Audit Trail (CAT)

As the Securities and Exchange Commission and self-regulatory organizations (SROs) move forward with the development of the Consolidated Audit Trail (CAT), SIFMA member firms want to ensure that the development of the CAT does not introduce new data protection risks. The CAT system was developed in response to the 2010 "Flash Crash" to improve regulators' ability to monitor market activity and identify manipulation and other illegal activities, but as currently designed, the CAT could also be a gateway for cyber criminals to access confidential trading information and the personal information of tens of millions of retail investors.

Once complete, the CAT will be the world's largest data repository for securities transactions, and one of the world largest databases of any type. Every day the system would ingest 58 billion records - orders, executions and quotes for the equities and options markets – and would maintain data on over 100 million customer accounts and their unique customer information. This data would grow to an estimated 21 petabytes within 5 years – the equivalent of over ten times the content of all U.S. academic research libraries, in a single database.

The current National Market System plan, developed by the exchanges and FINRA and approved by the Securities and Exchange Commission, raises serious concerns around data protection and the ability to confidently secure the critical information it will contain. One of our top concerns is that the CAT will hold massive amounts of personally identifiable information on retail investors who trade in the U.S. securities markets. The current CAT plan requires reporting firms to provide a significant amount of sensitive customer information, including name, social security number, and address. The CAT will also hold sensitive trade information, which could be used to reconstruct proprietary trading strategies. The database will provide regulators with the ability to aggregate information from all broker dealer and exchange CAT reporters. This information will be held in a single database that creates a high value target, and bad actors will have a strong incentive to find the weakest link to gain access. While our concern existed before the recent breaches, many stakeholders remain skeptical that the CAT, as currently designed, will be able to protect the massive amount of sensitive PII for every investor in America.

Importantly, just as the industry should and does consider whether sensitive information needs to be collected and retained for a particular purpose, so too does the case need to be made that PII is required to be collected and reside inside the CAT for effective surveillance.

The range and scale of data stored in the CAT alone would raise data protection concerns, but the current proposed policies for securing and accessing the database are not adequate. The NMS plan which lays out requirements for the CAT system requires that the system support a minimum of 3,000 users. Twenty-two different SROs as well as the SEC will have access to the CAT trading data. Under this configuration, it will not be enough to secure data held within the CAT system itself. Rather, every user with access to bulk downloads of sensitive data, across every participant SRO, will need robust security protections as well.

Despite these serious data protection concerns, the CAT technical specifications that have been released to date include alarmingly few details on data security and protection. In addition, SIFMA is concerned that an unreasonably tight timeline, which is based on arbitrary dates as opposed to the proper time needed for effective development, will not allow for adequate time to implement the necessary cybersecurity and data protection measures.

Given the sensitivity of the information held by the CAT on securities markets and retail investors, we believe that the design and development process of the system needs to ensure it is completely secure against breaches and data loss – and the system requirements and development timeline should be oriented to make sure this critical goal is achieved.

Importance of Regulatory Harmonization

Over the past two years regulators in the U.S. and around the world have proposed or finalized over 30 new cyber rules and regulations applicable to the financial services industry. While regulations can help raise expectations and define strong standards for market participants, the volume of regulations have resulted in requirements which are sometime overlapping, duplicative and conflicting.

Consider that for the financial services industry there are no fewer than 11 federal agencies that impose some form of cybersecurity requirements. This is in addition to individual states' requirements and those of self-regulatory organizations such as the Financial Industry Regulatory Authority and the National Futures Association. These rules and guidelines are further layered with standards developed by the National Institute of Standards and Technology and the International Organization for Standardization, which guide financial institutions in setting cybersecurity standards and measuring the adequacy of cybersecurity programs. Large financial institutions may also be subject to additional or different cyber regulations in each region where they conduct business.

As the number of different regulations increase, so to do the resources firms need to spend to demonstrate compliance. When the process of rule writing at agencies is not coordinated, the risk of different definitions, measurement standards, and technical requirements proliferate, creating administrative burdens for firms. Some large firms report that approximately 40 percent of their corporate cybersecurity activities are focused on compliance rather than security, where their time and resources could be better spent building even stronger defenses and better resiliency and recovery.

In recognition of the cyber threat to the financial sector, a coalition of financial services trade associations and the Financial Services Sector Coordinating Council (FSSCC), working with SROs, state regulatory agencies, and members of the Financial and Banking Information Infrastructure Committee (FBIIC) agreed to create forums to discuss various guidance, tools, frameworks, regulations and examination processes, built around the NIST Framework.

Regulators could help enhance defense and resiliency by establishing a unified cyber assessment framework and common set of controls across financial services regulatory bodies. The use of consistent language and terminology in regulations, guidance, rules and examinations would go a long way in promoting efficient cybersecurity spending. The cybersecurity standards developed in 2014 by the National Institute of Standards and Technology could form the basis of this common framework.

To their credit, regulators should be recognized for making strides towards harmonization, including the formation of a Regulatory Harmonization Working Group. The industry also welcomed the President's May 2017 Executive Order calling for a comprehensive review of cybersecurity efforts across all government agencies.

In parallel with the joint-trades effort, SIFMA and our affiliated non-U.S. organization have advocated for the global use of the NIST Framework and the industry is developing a financial sector version of NIST to encourage global adoption.

This harmonization of regulations and a common framework is essential to simplify the process of compliance and allow financial institutions to dedicate the right resources to protecting their institutions and securing sensitive data.

Penetration Testing

As firms and regulators look to improve their data protection and cybersecurity programs, many have recognized the value of penetration testing, as previously mentioned. Penetration testing allows firms to evaluate their systems and the controls that protect them, to identify and remediate vulnerabilities, and use these findings to strengthen their infrastructure against current cyber threats.

Regulators and supervisors internationally have also shown increasing interest in incorporating penetration testing into their cybersecurity oversight programs. This has led to the creation of multiple regulator-guided pen testing initiatives.

Despite the value of penetration testing in identifying vulnerabilities which firms can then correct, duplicative regulator-initiated tests may unintentionally increase risks to the financial services institutions. These risks could include:

- Damaging firms' production information security environments;
- Sharing of firm's sensitive test results data with third-parties increases the risk the firm will lose control of that data; and
- Forcing firms to spend more time on compliance and less time developing defensive measures to protect the organization's infrastructure.

Beginning in the first-quarter of 2017, SIFMA, working with its regional partners the Association for Financial Markets in Europe (AFME) and the Asian Securities Industry and Financial Markets Association (ASIFMA), organized through the Global Financial Markets Association (GFMA) led a global advocacy campaign to address the impacts of penetration testing on the safety and security of the financial sector and the need for a scalable sustainable way forward.

Our ideal end-state for this initiative is for regulators and supervisors to permit firms to test internally, or use external testers of their choosing. To ensure the quality of these tests, a firm's primary regulator would be involved in the scoping and scheduling of tests, and firms will provide regulators with confidence that tests are conducted by accredited certified professionals. Test results will not leave the subject financial institution; the full results can be viewed in-house at the firm by their primary regulator, with a summary of the results available to other regulators.

SIFMA and our affiliated organization have created a draft framework and white paper to outline a global firm-led testing framework to recommend best practices for conducting penetration tests. In this framework, we recommend principles that penetration testing regulations should provide primary regulators the ability to guide penetration testing programs at a high level, with common scenarios, scheduling and scope of testing activities. Regulators would also have transparency into

testing process and governance for both regulator-driven and firm-driven testing, as well as assurances that identified weaknesses are properly addressed. Furthermore, it would ensure testing activities are conducted in a manner that minimizes operational risks and enforces strict protocols for handling test findings due to the highly sensitive nature of this information.

Insider Threat

One of the greatest threats to our members' cybersecurity comes from within the firms – either current or former employees or others who have access to the firm's data. With the computerization of firm systems and assets, attacks can now be launched on a larger and more destructive scale than ever before. Insider attacks on firms' electronic systems can result in financial and intellectual property theft and the loss of sensitive client information, as well as firm-wide disruption to internal systems and customer operations. A recent Data Breach Investigation Report from Verizon shows that nearly 20% of breaches are caused by insiders and that almost 90% of breaches were motivated by financial gain or espionage.[5] Preventing and detecting insider attacks, is essential as insiders often look to capitalize on their familiarity with firm systems to instigate attacks and compromise data without attracting notice. A systemized, targeted program is therefore necessary to mitigate the insider threat.

While insiders take advantage of weaknesses in technical systems, insider threats are, at their core, a human issue. Cybersecurity defenses focused on monitoring employee activities may prevent some attacks from causing significant harm to an organization. Human intelligence, monitoring and managerial oversight are necessary to identify the potential warning signs of insider activity and the appropriate method to intervene before an attack occurs. An effective insider threat program uses both cybersecurity defenses and intelligence personnel to detect and contain insiders who pose a risk to the firm and mitigates the risk through administrative, investigative, technical or disciplinary safeguards and responses.

SIFMA works to support firms as they develop their insider threat prevention programs – by building dialogue between our member firms and the public sector, academia, and technology firms,

[5] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

benchmarking of best practices, and developing best practice guidance to help firms build out a robust insider threat management program and to understand the legal context that shapes what is permissible.

Exercise Programs

As firms continue to develop their cybersecurity and data protection programs, we believe that sector wide exercises are a critical tool to help firms and regulators exercise their playbooks, learn to work together, and continue to find opportunities to improve their preparation and training. The lessons and experience firms develop during exercises help make themselves more secure and develop the muscle memory needed to quickly respond in the event of an actual cyber incident.

SIFMA has organized a series of sector-wide cyber exercises since 2011. These "Quantum Dawn" exercises have provided a forum for firms, regulators and law enforcement to exercise their playbooks, work together to respond to simulated cyber incidents, and identify opportunities to improve. With scenarios ranging from attacks on the equity markets to clearing and settlement disruptions to data breaches, these exercises have helped the industry learn and develop their capabilities. The latest exercise in the series, Quantum Dawn IV, will focus on exercising the industry's ability to respond and recover from a targeted systemic cyberattack affecting multiple financial institutions, and how firm, sector, and government playbooks would support this process. The exercise will bring together nearly 60 financial services firms, exchanges, and utilities.

SIFMA and its member firms have also participated in a public-private exercise program, the Hamilton Series of cyber exercises, which brought together firms, trade associations, and U.S. government agencies to better prepare the financial sector to address the risks and challenges presented by significant cybersecurity incidents. The exercises range from regionally-focused events among small and medium-sized companies to cross-border tabletops, to sector-wide exercises. These scenarios examined impacts across different segments of the financial sector, including impacts to equities markets, depository institutions, payments systems, liquidity, and futures exchanges. The lessons learned from these exercises have helped the industry and our government partners identify what new initiatives would be most effective in continuing to improve the

industry's cyber and data protection policies, and where we can work together to help protect each other and our clients.

Sheltered Harbor

While the industry is committed to securing the sensitive data it has been entrusted with, we also plan for all contingencies including potential successful cyber-attacks. As part of regular joint government-industry exercises, we determined the need to develop a system to provide for the restoration of customer data when records are erased and systems compromised. The industry has organized a program called "Sheltered Harbor" to give the sector a protocol to safely secure retail customer demand deposit and brokerage accounts off site or off line in a standard recordable format.

Firms participating in Sheltered Harbor will be able to securely store and reconstitute their end of day customer account information, through a service provider or other firm, if they are unable to recover from a cyber incident in a timely fashion. All participating institutions, on a regular basis, will make a copy of the consumer's end of day account data in a standard format, which enables the restoration of accounts in the event of a major outage. The account data is archived in a secure data vault that is protected from alteration or deletion. The data will stay intact and accessible if needed - exactly as when it was archived. Sheltered Harbor is expected to be fully operational in 2018. Sheltered Harbor further aligns and compliments a joint securities industry regulator effort to ensure customers remain connected with their assets should a broker dealer experience financial difficulty through a swift transfer of that broker dealer's customer accounts to another broker dealer, and the subsequent reestablishment of the client relationship.

Conclusion

Effective cybersecurity will be in a state of discussion and improvement for years to come. That security is a combination of activities that relies on strong defenses, information sharing, mitigation and recovery planning. It can only be accomplished through constructive dialogue and engagement among the private sector, policymakers, and regulators. Much work has been done but as this

testimony lays out, there is much more work to come. SIFMA and its members stand ready to do their part.