Testimony of Russ Fitzgibbons, Executive Vice President and Chief Risk Officer
The Clearing House Payments Company
Before the House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit
"Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats"
May 19, 2015

Good afternoon Chairman Neugebauer, Ranking Member Clay, and members of the Subcommittee. My name is Russ Fitzgibbons and I am the Executive Vice President and Chief Risk Officer of The Clearing House Payments Company L.L.C. (The Clearing House). As Chief Risk Officer, I am responsible for enterprise risk management, information security, and business continuity. I also serve as the current Chair of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). I appreciate the opportunity to appear before you today to discuss issues that are critical to all Americans—the protection of our payments systems against cyber threats.

The Clearing House is the nation's oldest banking association and payments company, founded in 1853 and owned by twenty-six banks. Our mission is to ensure the safety, soundness, and efficiency of the payments system in particular, and to enhance financial stability more generally. The Clearing House provides payment, clearing, and settlement services to our owner banks and other financial institutions, clearing and settling nearly $2 trillion daily. The Clearing House's owner banks collectively hold over 55% of the nation's deposits; issue over 40% of debit cards; and issue over 70% of Visa and MasterCard-branded cards. The Clearing House also engages in payments technology and payments systems security advocacy.

The Clearing House operates the Clearing House Inter-bank Payments System (CHIPS) and the Automated Clearing House (ACH). We are the only private-sector ACH operator in the country, processing approximately 50% of all commercial ACH volume in the United States through our networks. CHIPS is the largest private-sector U.S.-dollar

funds transfer system in the world, clearing and settling an average of $1.5 trillion in payments—both domestic and cross-border—daily.

The Clearing House also seeks to leverage its core capabilities to enable innovation across the sector. We regularly work with our owner banks and others to develop next generation payment systems—with the same safety and soundness principles that have always underpinned our core systems. For example, we are currently working to deploy a tokenization platform to enhance the security of credit and debit card transactions, including those made online, and developing a real-time payment system.

Because of the volume and importance of the financial transactions enabled by The Clearing House's systems, robust protection of those systems from cyber threats is essential.

Cyber threats to banking infrastructure have become more frequent and more sophisticated in recent years. The criminal organizations and other groups launching these threats are constantly innovating, and we need to be at least as agile as they are in defending ourselves.[1]

I will divide the remainder of my remarks into three areas:

A. **Financial Sector Efforts:** Ways in which financial institutions such as The Clearing House are working to defend ourselves against cyber threats, including through technological innovations and cooperation within the private sector;
B. **Strengthened Collaboration Between the Private Sector and Government:** The crucial role that strengthening our partnerships with government can and must play in further enhancing the security and resilience of our payments and financial systems;
C. **Legislative Assistance:** Areas where action by Congress could help both the financial services sector and our government partners work even more effectively to advance our common goal of strengthening the financial sector's resilience in the face of cyber attacks.

A. <u>Financial Sector Efforts</u>

Let me begin by discussing some of the ways in which financial institutions work to defend themselves and their customers against cyber threats, both on their own and frequently in collaboration with other financial services firms and industry organizations.

[1] See, e.g., Cedarbaum and Reilly, Cybersecurity Collaboration: Routes to Stronger Defenses, Banking Perspective (Q1 2015) at 68-69.

First, as you know, financial institutions have been subject to the requirements of the Gramm-Leach-Bliley Act (GLBA) for roughly a decade and a half. The GLBA requires financial institutions to adopt "administrative, technical, and physical safeguards" that help ensure the "security and confidentiality of customer records and information," "protect against any anticipated threats or hazards to the security or integrity of such records," and "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[2]

Financial institutions are also subject to other special legal and regulatory requirements such as those promulgated by the federal financial regulatory agencies of the Federal Financial Institutions Examination Council (FFIEC). For example, the FFIEC has issued "Interagency Guidelines Establishing Information Security Standards" (Interagency Guidelines), which direct financial institutions to implement "a comprehensive written information security program." Financial institutions' information security programs must include five basic components, including oversight of service providers. Pursuant to these requirements, The Clearing House's data security practices are subject to regular examination and supervision through the FFIEC's Multi-Regional Data Processing Servicer Program (MDPS).

As threats to our payments infrastructure evolve, so too do our defenses. Technological innovation is an important weapon in our arsenal. One example of innovation that is being readied for deployment is Secure Token Exchange, a new platform of The Clearing House which replaces account numbers with randomly-generated temporary numbers during processing. With Secure Token Exchange, the customer's actual account information is not transmitted outside of banks and their service companies. This type of anonymization provides a layer of security for customers, merchants, and banks while preserving the current customer experience. Secure Token Exchange reduces the risk of cyber criminals being able to gain access to customers' financial information because the information exists only behind the firewalls of highly regulated and supervised financial institutions and their service companies. Over the coming months and years we will be transitioning credit and debit card payment transactions to Secure Token Exchange. We believe this model is scalable to other facets of the payments system, including ACH transactions and the real-time payment system currently under development by The Clearing House.

Effective cybersecurity requires more than technological innovation and sophistication. It requires organizational dexterity and agility as well. Like many other financial institutions, The Clearing House has made training and exercises an increasingly important component of our cybersecurity efforts. Just to give one example, the Financial

[2] 15 U.S.C. § 6801(b).

Services Information Sharing and Analysis Center (FS-ISAC), has for several years held an annual two-day simulation known as The Cyber Attack Against Payments Processes (CAAPP) designed to enable companies such as The Clearing House to put their cyber defense processes to the test and thus identify areas for improvement.

Effective cybersecurity also requires awareness and early warning of potential threats and risks. In part, we do this by participation in information-sharing programs. Our primary mechanism is via the FS-ISAC, which has over 5,000 member organizations and has become an operational information-sharing model for other sectors. It has found a good balance of member-to-member and sector-wide sharing of threat analysis information, vulnerability data and indicators of potential problems. Of particular note, FS-ISAC enables institutions to share information anonymously.

FS-ISAC members, which range from small community banks and credit unions to some of the largest financial institutions in the world, make contributions to the information-sharing effort commensurate with their resources and capabilities. Large bank members, which by and large have substantially greater resources to devote to threat intelligence collection and other information-gathering efforts, play a particularly important role, and their contributions benefit the entire sector, as they are disseminated through the FS-ISAC platform.

There are several types of information that are shared with high frequency, including:

- Identity of servers used by malicious cyber actors and the routes over the internet they use to deliver their attacks;
- Malware and other threat signatures, which are used for scanning networks to detect the presence of threats;
- Attack vectors, which are paths for gaining access to a system; and
- Situational awareness intelligence.

As the volume of threat activity has grown, the need for effective automated information-sharing has become crucial to ensuring that financial companies can respond rapidly to the shifting threat environment. Enabling efficient and time-sensitive information-sharing is a priority at the highest levels of our member banks, with two CEO's taking the industry lead to ensure that this effort is fully realized.

Through FS-ISAC and Depository Trust & Clearing Corporation (DTCC), the sector recently deployed a more effective platform for real-time automated sharing of cyber threat information called Soltra Edge. Utilization and integration of Soltra Edge across the sector's infrastructure are expected to grow significantly over the next few years.

Cross-sector information-sharing can also make an important contribution to cybersecurity. Thus, the FS-ISAC and others have been working with other sectors (e.g., energy, telecommunications, retail and legal sectors) to join forces in information-sharing efforts.

B. <u>Strengthened Collaboration Between the Private Sector and Government</u>

In response to the growing cyber threats we face, financial institutions have dramatically increased their own investments in cybersecurity defensive measures. But comprehensive cybersecurity requires that the federal government use its authority and capabilities to proactively mitigate threats and work with the financial community to employ defensive measures. Addressing the cybersecurity challenge requires a team effort. We must be data driven in our assessment of threats and risks and prioritize accordingly. We must also maintain and enhance the collaboration and teamwork that happens in the sector today. Our efforts must scale at the same pace or faster than the risks our networks face.

Through FS-ISAC and other organizations, we coordinate closely with the National Infrastructure Coordinating Center (NICC), the Department of Homeland Security operations center that maintains awareness of critical infrastructure for the federal government and law enforcement agencies. We actively participate in the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), of which, as I previously mentioned, I am currently the Chair. We also work closely with the Treasury Department's Office for Critical Infrastructure Protection and Compliance and its Cyber Intelligence Group.

In my estimation, the goodwill between government partners and the financial sector is at an all-time high. There is an increased sense of urgency, the operations tempo is improving, and the depth of information shared is much better than in the past. One notable example is the effort to streamline the process for financial companies to request technical assistance from the government in responding to cyber threats. This joint effort between the Securities Industry and Financial Markets Association (SIFMA), other trade associations, various government agencies, and several financial firms will help to improve collaboration between the financial sector and our government counterparts during cyber incidents. This effort helps the sector become more resilient.

While the financial services sector has made considerable strides in its sharing within the sector and with our government partners, there are still areas for improvement. Companies in the financial sector share information quite extensively with the government, and the flow of information from government agencies to the private sector has increased significantly. But we have lots of opportunity to improve our ability to support our cyber first responders, defend critical infrastructure, and protect our stakeholders. The

Administration has issued two executive orders designed to improve the government's sharing of information with the private sector, and there have been resulting improvements. However, more work needs to be done on the analysis and contextualization of threat information, and government agencies need to continue increasing their prioritization and allocation of resources for declassifying information that pertains to network defense.

We also need more affirmative efforts by the government to defend the private sector against cyber threats, especially those emanating from abroad. To the extent lack of certainty about the government's legal authority to act has hampered government action, those authorities should be clarified. A good example of this is included in the Administration's cyber legislation proposal. "One powerful tool that the [Justice D]epartment has used to disrupt botnets and free victim computers from criminal malware," the head of the Justice Department's Criminal Division has noted, "is the civil injunction process."[3] "The problem is that current law only permits courts to consider injunctions for limited crimes."[4] The Administration's current legislative proposal would add operation of a botnet to the list of offenses eligible for injunctive relief, thus clarifying the government's ability to use civil injunctions to go after cyber criminals and shut down botnets, which are often used as platforms for attacks on financial services companies.

C. Legislative Assistance

We also believe that Congress has a role to play in promoting greater and more effective cybersecurity. Information-sharing efforts have greatly improved in recent years and already make an important contribution to the financial sector's cybersecurity. But concerns about various forms of liability exposure resulting from information-sharing continue to make information-sharing less vigorous than it should be and thus weaken our sector's cybersecurity capabilities. The Justice Department's recent white papers on antitrust and Stored Communications Act issues have helped address some of those concerns. Others, however, remain. Thus, action by Congress to pass comprehensive cyber threat information-sharing legislation with protections against liability for companies that collect and share in accordance with the law is essential.

We agree with our financial services counterparts and support both bills passed by the House in April: the National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731), and the Protecting Cyber Networks Act (H.R. 1560). We also support the leading Senate bill, the Cybersecurity Information Sharing Act of 2015 (S. 754). However Congress

---

[3] Assistant Attorney General Leslie R. Caldwell, Assuring Authority for Courts to Shut Down Botnets (Mar. 11, 2015), available at http://www.justice.gov/opa/blog/assuring-authority-courts-shut-down-botnets.

[4] *Id*.

decides to move forward with these bills, we believe that any final legislation that is sent to the President must accomplish the following:

- Facilitate real-time sharing to enable institutions and governments to act quickly;
- Provide liability protection for cyber threat sharing within the private sector and between the private sector and the government;
- Provide liability protection for system monitoring and other essential self-defense measures companies take on their own networks;
- Provide protection from disclosure of information shared with the government through the Freedom of Information Act (FOIA) and limit the use of such information to cybersecurity purposes;
- Facilitate the appropriate declassification of information by the intelligence agencies and expedite issuance of clearances to private sector individuals;
- Include appropriate privacy protections, especially for personally identifiable information (PII); and
- Clarify the government's authorities to take action to defend the private sector.

Thank you for your attention to this critically important issue and for the opportunity to testify today. I look forward to answering any questions you may have.