WRITTEN TESTIMONY

BEFORE THE

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

HEARING ON

"THE GROWING CYBER THREAT AND ITS IMPACT ON AMERICAN BUSINESSES"

MARCH 19, 2015

9:00 A.M.

TESTIMONY OF

JOHN LATIMER

CHIEF RISK AND COMPLIANCE OFFICER

TOTAL SYSTEM SERVICES, INC. (TSYS)

Introduction

Chairman Nunes, Ranking Member Schiff, and members of the committee. My name is John Latimer and I am the Chief Risk and Compliance Officer of Total System Services, Inc. (TSYS). In my capacity as Chief Risk and Compliance Officer, I am responsible for both logical and physical security, risk and compliance, operational and regulatory compliance, business continuity and disaster recovery, and encryption services. I appreciate the opportunity to be here today to discuss the important issues surrounding cybersecurity, cyber-crime, and data protection.

TSYS is a worldwide leader in the credit card and electronics payments industry with more than 10,000 employees. We serve nearly 400 card-issuing clients in 85 countries and more than two million merchants in all 50 US states. We believe that ensuring the ability of consumers to have access to all aspects of the non-cash payments space today is not only a personal issue, but a national security issue. Every day, we operate behind-the-scenes to route money from payment cards so that hundreds of millions of consumers and small businesses may have secure and convenient alternatives to cash and checks. Our familiarity and interaction with cybersecurity literally predates the Internet as we have been providing the systems that route money from consumers and merchants to payment networks, financial institutions, and retail businesses through a broad range of payment technologies for more than four decades.

At TSYS, we believe that people come before profit and "people are at the center of our business." We understand that in today's world of electronic payments, the more than 700 million credit, debit, private label, and prepaid cards we process provide cardholders over the globe the ability to make cashless payments for gas, groceries, clothes, and other needed services. In many cases it also gives cardholders the ability to meet emergency needs such as the unexpected medical expense, car repair, or the need to buy an airline ticket when a loved one is taken ill. Thousands of merchants also depend on us to ensure they are able to quickly and accurately accept electronic payments, either in person or over the Internet. Our systems

As a pioneer in the payments processing space, TSYS has contributed significantly to the worldwide transition to a "cashless economy." To give some idea about the scale of this "cashless economy," it might be helpful to understand that TSYS alone clears and settles trillions of dollars and processes billions of transactions each year. Not surprisingly, since assuming duties as the TSYS Chief Risk and Compliance Officer nearly a decade ago, one issue – data protection – has eclipsed all of my other day-to-day concerns. At TSYS, nothing is more important than the trust of our clients, and this confidence is completely dependent upon our ability to protect their data from an ever-growing array of cyber-criminals.

My purpose today is to explain the types of threats we see every day, how we defend against these threats, and to discuss some suggestions for how the US Government might assist us with our responsibilities.

The Current Threat Landscape

At TSYS, we are fully aware of the fact that we are a target for cyber criminals, and that threats can originate both externally and internally to our corporation. Additionally, we understand that we are subject to an unfortunate paradigm where the protectors are often more vilified than the criminals. Whereas in the case of a bank heist the bank robbers are considered the "bad guys," if we have a data breach – the thieves are forgotten and we are left to absorb all the blame. Despite these two disadvantages, TSYS works diligently to detect, assess, and mitigate a myriad of cyber threats.

At TSYS, we spend millions of dollars each year protecting our infrastructure; however, the current cyber threat environment becomes more dangerous every day as attacks increase in number, pace, and complexity. Attacks today are no longer confined to a high school kid defacing a webpage, or isolated instances of fraud by unsophisticated criminals.

On a daily basis, we monitor and intercept the actions of a variety of actors – hackers, "hacktivists," criminals, and even nation/state-sponsored advanced persistent threats (APTs), which we believe include terrorist activities. Every day, our systems prevent thousands of malware attacks (e.g. viruses, etc.), block malicious intrusion attempts, and we utilize advanced

security systems and techniques that help us detect known and unknown "bad actors." Additionally, we observe the regular occurrence of social-engineering events such as email and telephone "attacks" aimed at executives and team members. And, given the myriad of different applications and hardware platforms involved in enabling our successful payments-processing, we must also monitor for risks such as a missed system patch or coding standard, which might leave us exposed.

Attempts against our infrastructure today take many forms. It may be an exploitable vulnerability in a piece of code, a malicious malware payload in an email, or a distributed denial of service attack. Every day we have thousands of attempts to penetrate our infrastructure which come from multiple sources with different intentions. Organized crime syndicates routinely challenge our defenses attempting to steal cardholder information for financial gain. Most of these attacks originate from former Soviet bloc countries as well as inside the US. Attacks against our infrastructure to manipulate, destroy, or steal data or proprietary information also come from a variety of nation state actors.

Internally, we use a Computer Security Incident Response Team (CSIRT) to investigate any indicators that may suggest we have a threat from within. Although we think we have a great team, with 10,000+ team members and a number of third-party contractors, our approach to internal cyber-vigilance leads us to assume that there is always a "bad apple" among the bunch. Our range of focus on internal threats is very wide, spanning from the accidental to the purposeful. Threats that we guard against internally include: the inadvertent disclosure of client information, the accidental misconfiguration of systems or applications, the loss or theft of company information technologies (laptops, tablets, phones, etc.), the disclosure of proprietary information via Social Media, and even the intentional exfiltration of Company documents or Client Data.

How we defend

To best protect ourselves against this variety of external and internal threats, we use a "defense in depth" strategy. Although a defense in depth does not, and cannot, stop attacks, it mitigates the effects of attacks by applying a layered, overlapping, and redundant approach to the

defense. In military parlance, it is like having a series of obstacles to slow an attacker while the defender responds to repel the attack. The defense-in-depth strategy is regarded as the industry standard.

We monitor these defenses through a set of persistent capabilities in our Global Threat Management Center that provides 24/7 security monitoring, situational awareness, intrusion analysis and defense-in-depth protection of client data and corporate assets from global threat actors. Employing a state-of-the-art Security Information and Event Management (SIEM) console, we are able to correlate hundreds of thousands of incidents into a centralized, holistic, and integrated view of actionable security events. This enables prioritization and clarity as we respond to security events.

As we see threats against our infrastructure, we routinely share this information with our peers in the industry. While we may be competitors in the marketplace, we are united in our efforts to combat threats against the payments space. Philosophically, we believe an attack against one of us is an attack against all of us. While most of our intelligence sharing is done through the Financial Services Information Sharing and Analysis Center or FS-ISAC, another organization which has been and continues to be incredibly effective in regards to the expeditious sharing of threat information, is the Payment Processors Information Sharing Council or PPISC, which is sponsored by the FS-ISAC. Rarely does a day go by that our team is not communicating with industry counterparts in the PPISC to discuss emerging threats and mitigating activities.

The financial industry has continued to enhance intelligence sharing with Soltra Edge, a threat intelligence-sharing platform created by a joint venture between FS-ISAC and the Depository Trust and Clearing Corporation, and funded by contributions from the financial services community. Soltra Edge enhances the current information-sharing model to make it more automated and collaborative so actionable intelligence from multiple sources can be disseminated in near real time, allowing organizations to more effectively counter cyber threats.

Our concerns

At TSYS, we think there are four significant cybersecurity policy issues worthy of consideration by this committee: the protection of critical infrastructure, policies regarding information sharing, data breach reporting, and data breach liability.

Protection of Critical Infrastructure: As the threat of terrorism has increased, so has the need to identify and protect areas where terrorist acts have the greatest impact. Historically, these include attacks in public forums (e.g. Atlanta Olympics), against noteworthy physical facilities (e.g. World Trade Center), and reduction of services (e.g. postal delivery of anthrax). In this regard, we believe an attack on the payments infrastructure could have an even more significant direct and emotional impact on a population conditioned to using credit / debit cards for virtually all purchases (e.g. gas to groceries) and payments (e.g. bill-pay services) … and significant negative impact on retailers who have gradually become ill-equipped to deal with offline payments.

Specifically, critical infrastructure supporting the payments space, as described within the US Government's (USGs) "Framework for Improving Critical Infrastructure Cybersecurity" (Feb 2014), should be identified to determine nodal vulnerabilities, potential points of exploitation, and security enhancements identified with recommendations to infrastructure owners. Further, and where appropriate, provisions for government-sponsored incentives (tax credits) should be established for responsible businesses that expend private capital to mitigate nodal vulnerabilities or to strengthen existing infrastructure (e.g. harden; add redundancy; etc.). These incentives should be extended to all businesses who willingly prioritize efforts to achieve increased levels of cybersecurity preparedness.

Information Sharing: Regarding information sharing, TSYS agrees in principle with the benefits to be realized by industry-government information sharing regarding cybersecurity issues. As one of the founding members of the Payment Processors Information Sharing Council (PPISC), we have always been an advocate of peer information-sharing. The FS-ISAC does this today by gathering cyber threat information and disseminating threat alerts and critical information to members including analysis and recommended actions. FS-ISAC supported the establishment of

the Payment Processors Information Sharing Council with the mission of "bringing together stakeholders in the payments arena to develop solutions, identify best practices, and facilitate the exchange of information that will result in a more secure use of electronic payments and related practices." FS-ISAC is leading an initiative to automate information sharing using common frameworks (e.g. Soltra Edge).

Our view is that Government should continue to leverage the FS-ISAC and PPISC as distribution conduits for cybersecurity information-sharing as an efficient method of getting critical threat data to Financial Service Institutions (FIs). Furthermore we would encourage the Government to share cyber threat intelligence with the financial industry in a timely manner. To be clear, source intelligence requiring security clearances is not always needed; most times we simply need to know attack intentions and vectors to mitigate threats. In support of these actions, TSYS recognizes and is appreciative of Government efforts to streamline the process for industry security personnel to obtain "secret" clearances to receive and share information from / with law enforcement agencies (LEAs) and security agencies.

Data breach reporting: Regarding data breach reporting, TSYS supports current legislative efforts to establish a single, federal reporting standard which protects consumers, provides consistency for financial institutions and processors, and allows interaction with law enforcement agencies. The current complexity of reporting requirements increases difficulty of adhering to state requirements and increases risk of legal action and fines for financial institutions and processors, and the variations in notification requirements for portfolios which cross state lines does not provide consumers equity in the notification process. In some cases, breached parties may be requested by LEAs to delay notification to facilitate the tracing and apprehension of criminal elements.

Data breach liability: The current paradigm, in which data thieves and criminals "get a pass", while FIs and processors are portrayed as villains, is unhelpful to industry, the market, and the overall efforts at cyber-defense. Maintaining complete data security is not possible in the current threat environment. However, FIs and processors dedicate countless hours – and billions of dollars – trying to keep one step ahead of the cyber criminals. It is our view that FIs

and processors which employ industry security best practices and "pass" data security compliance assessments (e.g. PCI), should not be penalized for criminal actions which compromise PII or financial information. However, those which do not adhere to industry best practices / standards should be subject to the full level of liability. Additionally, Government should consider liability exclusion provisions / tax credits for financial institutions and processors which suffer a criminal breach and have demonstrated appropriate security practices and possibly look at the development of government sponsored "insurance" (e.g. like FDIC for consumer deposits) to cover notification costs and prohibit frivolous litigation where no processor culpability is indicated.

Conclusion

In conclusion, we believe protecting the payments space must be viewed as a national security priority and as such, all of us ... industry, law enforcement, intelligence agencies, DHS and even DoD ... must work together to counter the threats of criminals, rogue nation states, hactivists, and terrorists. We can no longer allow ourselves to be segmented because of security clearances and turf battles and we would solicit this committee to help remove these barriers to information sharing. This is especially important as the threat of terrorist activity against the financial services sector continues to increase.