May 14, 2015

Testimony of
Tim Pawlenty

On behalf of

The Financial Services Roundtable

Before the

United States House of Representatives
Committee on Financial Services

Hearing on

"Protecting Consumers: Financial Data Security in the Age of Computer Hackers"

Chairman Hensarling, Ranking Member Waters and Members of the Committee, thank you for having me here today.

On behalf of the members of the Financial Services Roundtable,[1] I appreciate the opportunity to discuss the challenges consumers and businesses face from data breaches and the growing need to enhance data security efforts. The entire financial services industry – from the diverse members of FSR to the approximately 14,000 community banks and credit unions in this country – are united on efforts to protect consumers and prevent the type and volume of incidents that led 2014 to be dubbed "the year of the breach."[2]

My testimony today will cover the following topics:

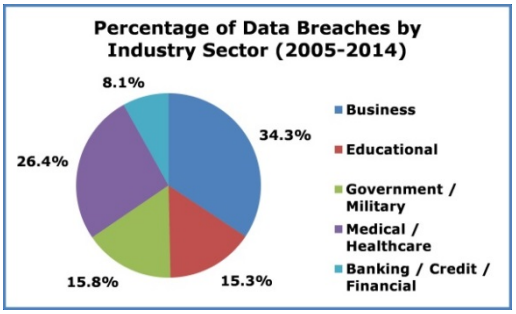
- A macro overview of data breach trends;
- How the payments system is evolving, and the importance of forward-looking security and technology;
- The clear need for Congress to enact "bank-like" data security requirements for all industries and common-sense consumer breach notification standards; and
- How current legislation, the Data Security Act of 2015 (H.R. 2205), accomplishes these goals by providing the highest level of consumer protection found in any bill currently introduced in the House.

Data Breaches: An Ongoing Challenge

No entity is immune to hackers. There's a common saying that there are two types of businesses: those who know they've been hacked, and those that have been hacked and just don't know it yet.

Not surprisingly, financial institutions are a common target. As the data in Figure 1 show,

Figure 1



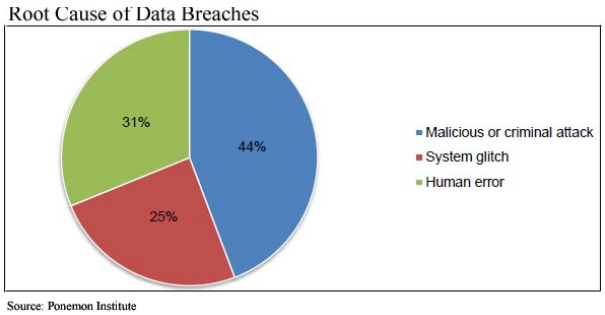
Source: Identity Theft Resource Center

[1] The Financial Services Roundtable represents the largest integrated financial services companies providing banking, insurance, payment and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. FSR member companies provide fuel for America's economic engine, accounting for $92.7 trillion in managed assets, $1.2 trillion in revenue, and 2.3 million jobs.

[2] http://www.infosecurity-magazine.com/news/2014-the-year-of-the-data-breach/

however, they seem to do better than any other major sector at defeating most of those attacks. Financial institutions accounted for only 8.1%[3] of data breaches in the U.S. between 2005 and 2014. Such results can be attributed, in part, to how the industry has adjusted to the changing cyber landscape. For example, the collaborative, real-time threat information sharing facilitated through the Financial Services – Information Sharing and Analysis Center (FS-ISAC) – a public-private partnership between financial services providers, commercial security firms, law enforcement and all levels of government – allows the industry to maintain the highest levels of threat preparedness and rapid response capabilities in the private sector.

Figure 2



As Figure 2 shows, data breaches occur for many reasons and in many ways.[4] "Phishing scams" are one common method hackers employ to gain access to systems. Such scams were a common entry point in several high-profile data breaches at retailers last year. Those scams allowed access to one portion of retailers' network infrastructure and that access eventually allowed the criminals to inject malware into point-of-sale systems to skim payment card data.[5]

Hacking methods aren't always that sophisticated, however. A simple unlocked door granting unauthorized access to a server, or a misplaced USB drive containing a spreadsheet of customers' sensitive information are also recent examples of how systems were breached and sensitive information was exposed. Many data breach incidents are preventable if proper safeguards and controls are in place.

Data breaches of sensitive financial information are, of course, costly for all parties involved. For example, financial institutions often bear much of the costs after a breach involving debit or credit cards, including the cost of card reissuance, covering fraudulent charges to uphold "zero liability" protections for customers, and reputational damage that is associated with a breach. The breach that occurred at Home Depot last year is estimated to have cost the credit union and community banking industries alone $60 million[6] and $90 million[7] respectively. A single large issuer may spend over $10-$20

[3] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html
[4] "2014 Cost of Data Breach Study: United States," Ponemon Institute. May 2014.
[5] http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/
[6] http://news.cuna.org/articles/53M_email_addresses_stolen_in_HD_breach,_impact_on_CUs_mounts
[7] http://www.icba.org/news/newsreleasedetail.cfm?ItemNumber=189537

million to reissue a portfolio of millions of card to mitigate just one major retail data breach.

The Fast-Evolving Payments System

Payment technology is rapidly evolving, and the financial services industry is driving much of the investment and innovation that will shape the future payments system.

In the near-term, cards will be much more difficult to counterfeit through the use of computer chips embedded in the cards as well as "tokenization" technology to make stolen data virtually worthless to criminals. In the future, new methods of identity verification that not long ago were the stuff of Hollywood movies – voice, facial recognition, biometric, location verification, gesture and behavior-based authentication, and more – will likely reduce or eliminate the need for traditional PINs and passwords.

Mobile payments, while still a small percentage of overall transaction volume, have gained great momentum in the marketplace and they will soon represent a significant portion of payment volume. Innovation and investment in payment security will increase as consumer adoption of mobile payment systems increases.

As policymakers consider a legislative response to data breaches, it is important to remember that no single card technology will prevent all data breaches. Effective defense strategies will require prevention across the entire interconnected payments system, not just one area or element of that system. Industries need to be holistic in their approach and parties to a payment transaction should layer security technologies to keep customers as safe as possible.

U.S. Migration to EMV

Later this year, a significant portion of the payments industry will undergo a fundamental change. Card networks have announced that starting in October, card issuers and merchants that implement certain stronger security technology will not be liable in the case of fraud, while companies that do not implement such advanced technology could be liable for fraud.

The technology driving this liability shift is EMV -- an acronym for Europay, MasterCard, Visa – which is a technical standard that enables chip cards to effectuate a more secure transaction. EMV chip cards are effective at preventing card counterfeiting, which helps reduce the amount of card-present fraud following a data breach of payment card

account numbers or other sensitive information.[8] However, EMV does not help prevent online fraud where a card is not physically used.

Many other countries have already moved to wide-scale EMV card acceptance. The reasons why the U.S. is just now making the shift to EMV chip card technology are worth reviewing.

The U.S. card market is somewhat unique in ways that make the shift to EMV more challenging. For example, most other EMV markets do not have 14,000 financial institutions and tens of millions of merchants that need to move in relative unison to implement EMV. Furthermore, the total volume of non-cash transactions in the U.S. is double that of the *entire* Eurozone.[9] So, the magnitude of the change is different in the U.S. and that change requires a significant overhaul of current systems. In considering those needed changes an industry representative stated the migration to EMV "…is comparable to declaring that U.S. drivers will now drive on the left-hand side of the road and changing all the road signs and highway entrance and exit ramps and reprogramming all the GPS systems."[10]

In any event, the changeover to EMV is now being implemented in the U.S. and its benefits will soon be available to American consumers and businesses.

Thinking Pragmatically about PINs

As policymakers contemplate federal policy regarding the future of payment security and related consumer protection, numerous factors should be considered. One such factor is recognizing government is not well-suited to predict or pick optimal future technology. Payment technology is changing and improving very rapidly. A government embrace of any one particular technology or approach is likely to limit more and better options as new technologies in this space now seem to emerge nearly each week.

- <u>50-year-old technology should not define the future of payment security:</u> Magnetic stripe technology was invented in the 1960s and it revolutionized the payments system at the time. PIN technology was also invented in the 1960s.[11] Both magnetic stripe and PIN technologies are dated and they are understandably being passed by more forward-leaning payments security technology.

[8] http://usa.visa.com/personal/security/chip-technology/emv-chip.jsp
[9] Capgemini *World Payments Report 2013*.
[10] http://arstechnica.com/business/2014/08/02/chip-based-credit-cards-are-a-decade-old-why-doesnt-the-us-rely-on-them-yet/
[11] See http://news.bbc.co.uk/2/hi/business/6230194.stm

In addition, it is important to remember that most merchants do not even currently accept PINs. According to the Federal Reserve, only 25% of merchants accepting debit cards accept PIN-based debit transactions.[12] According to point-of-sale (POS) hardware manufacturer Ingenico, of the nearly 3 million POS terminals at large merchants, nearly all have PIN capability. On the other hand, virtually none of the 22 million "micro merchants" have the current capability to accept PINs. Obviously, there is a big gulf between large and small merchants in their ability to accept PINs.

- Banks and retailers are moving to more secure forms of authentication beyond PIN: Payments innovators are abandoning static data elements in favor of dynamic, single-use technologies that can render stolen data useless to criminals. Financial institutions are also continuing to develop new ways to authenticate customers that don't rely on just one factor, like a password or a PIN. Biometric authentication is becoming an integral part of mobile payments, and other technologies focused on multiple factors, including gesture or behavior-based authentication, are being considered to help secure access to sensitive systems and transactions. BITS, the technology policy division of FSR, is collaborating with its members in the High Assurance Authentication Project which will help define optimal financial services technologies and practices for stronger authentication techniques.

  As consumers, most of us have probably noticed that more and more transactions don't even require a signature, let alone a PIN. According to data from Visa, more than 60% of Visa's U.S. transaction volume qualifies for no customer verification method at all because they are low-dollar and low-risk.

- No "silver bullet" has yet been developed to fully stop payment breaches and related fraud: In countries where EMV chip cards are utilized throughout their payments system, fraud rates from lost, stolen or counterfeit use at the point-of-sale have declined. However, after the introduction of EMV cards, in many instances overall fraud rates increased significantly due mainly to very large increases in card-not-present (CNP) fraud (i.e., online shopping).[13] Technologies are being developed to better address fraud in CNP situations.

[12] Federal Reserve Board of Governors. *Regulation II, Final Rule.*
[13] See Appendix 1.

Looking Forward in Payment Security

More innovation is taking place in payments than arguably in any other aspect of financial services. From increasing security and reducing fraud to creating a more friction-free experience for consumers, the financial services industry is committed to maintaining its role as consumers' trusted source for payments and managing money. With the support and drive from the financial industry, biometrics, cloud-based technology, location-based services, and keystroke behavior patterns will be the norm in the future. More immediately, the development of tokenization-- the process of replacing sensitive financial information with data that can only be interpreted by a very limited set of parties in the transaction chain-- is paving the way for mobile payments to become viable.

Transactions using tokenization help ensure stolen data is of no value in a data breach. Tokenization, along with biometrics or other layered security measures, help create a more secure mobile payment experience. Again, there is no single panacea to preventing fraud and stopping data breaches.

Creating "Bank-Like" Security for Firms of All Sizes

Congress should pass legislation creating a strong, meaningful data security requirement for all companies that handle sensitive customer information but currently have no federal requirement to protect it.

The Gramm-Leach-Bliley Act (GLBA) (Pub.L. 106-102), enacted in 1999, directed the Federal Trade Commission and federal and state regulators with oversight of financial institutions to establish appropriate standards and processes relating to administrative, technical and physical safeguards to protect customer information.

For the financial industry, the GLBA is implemented and enforced by pertinent federal and state regulators. For example, the federal banking agencies establish information security standards for banks and regularly examine banks for compliance with those standards, while the Securities and Exchange Commission oversees broker-dealers and investment advisors and state insurance departments oversee insurance companies in this regard.

The GLBA's standards and processes apply to the smallest credit union or community bank as well as the largest financial firms in America. This is made possible by the flexibility built into the GLBA standards that allow adjustments for the size and complexity

of the financial institution, the nature and scope of its activities, and the sensitivity of the information it handles.[14]

Addressing Small Business Concerns

While a clear need exists for Congress to enact strong data security legislation, any standard or process Congress creates should not be prescriptive, inflexible or overly burdensome for small businesses. For the reasons outlined above, a flexible standard that is adaptable to both the size of the entity and the changing nature of data security technology is the most common-sense approach. Such a standard has served the financial service sector and its customers well.

Similar to small financial institutions, small businesses frequently rely on third party vendors to implement and maintain core business functions like payment processing and data security.[15] In addition to providing the service, compliance responsibilities would likely be delineated via contract with such vendors.

Most small and medium-sized businesses do not maintain data centers or other extraordinary in-house technology that would be likely to invite significant new compliance requirements were Congress to enact bank-like security process requirements. However, it is highly likely that third-party service providers, particularly payment providers, will pay closer attention to the controls even the smallest of businesses has in place to protect customer information.

For example, it is not unreasonable to expect any size business to password-protect systems with something more robust than "password" or "123456." If a small business has a server or PC on which it maintains customer files with sensitive financial information, it would be wise to implement physical safeguards, such as a lock on the door with limited access. If a small business has a wireless internet network, it should be required to have at least minimal security features.[16]

This list is not exhaustive but is illustrative of the basic nature of data security requirements that can help prevent breaches yet are too often absent today.

---

[14] See *Interagency Guidelines Establishing Information Security Standards.* Accessed at http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm

[15] See, for example: National Small Business Association, "2013 Small Business Technology Survey," accessed at http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf

[16] For example, the 2007 breach at nationwide retailer TJ Maxx was caused by an unsecured wireless network that allowed hackers clear access to payment card information. See http://www.zdnet.com/article/tjxs-failure-to-secure-wi-fi-could-cost-1b/

The Right Legislation is Needed

Enacting the right data breach legislation will create a framework of complementary federal requirements and self-regulatory standards, such as those put forth by the PCI Security Standards Council. FSR, and many others in the financial industry,[17] believe data security and notification legislation should include the following elements:

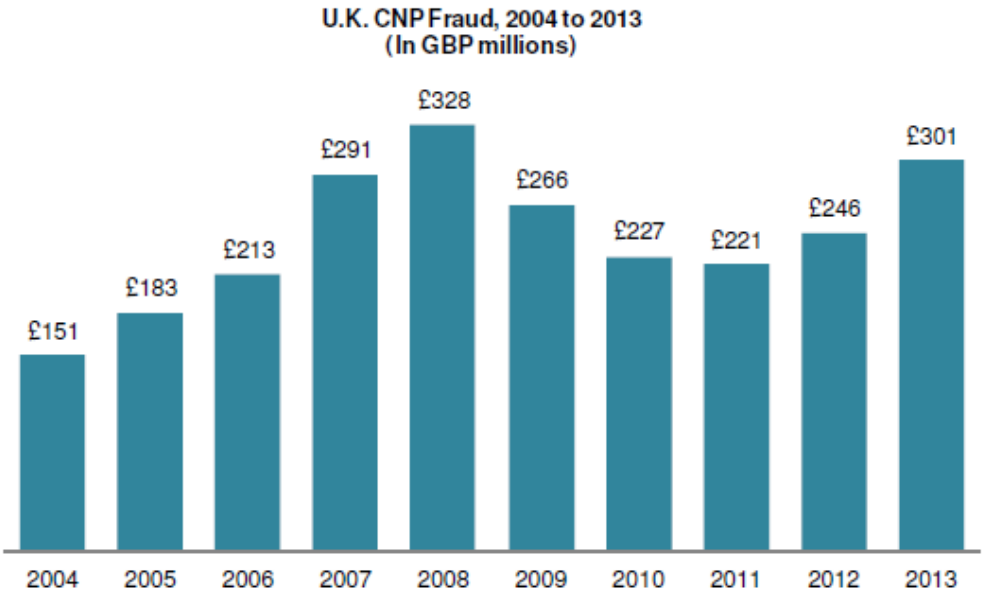
- A data security requirement establishing the framework for a flexible, scalable process firms should follow to implement administrative, technical and physical safeguards to ensure the security, confidentiality and integrity of sensitive consumer financial information.
- A common-sense notification process firms should follow in the event they discover a breach of information that could put consumers at risk of harm, and that ensures consumers are notified in a timely manner, but that allows for a reasonable delay for law enforcement investigation.
- Preemption of the patchwork of conflicting state data breach laws for all industries.
- A recognition that certain industries – like healthcare and financial services – already comply with federal data security and consumer notification standards, to ensure those industries are not faced with duplicative, unnecessary regulatory requirements.

Such provisions are contained in H.R. 2205, the Data Security Act of 2015, introduced by Congressman Randy Neugebauer and Congressman John Carney. *No other bill introduced in the House this session approaches the level of consumer protections contained in this measure.* Its provisions are reasonable, not overly burdensome on businesses, and will help stop the flow of data breaches. We encourage Members of this Committee to support this important measure along its path toward enactment.

Thank you for inviting me to testify. I look forward to your questions.

[17] For more information, see joint letter from FSR, ABA, CBA, The Clearing House, NAFCU, CUNA and ICBA: http://fsroundtable.org/fi-trades-sends-joint-letter-house/

Appendix 1



Source: Julie Conroy. "EMV: Lessons Learned and the U.S. Outlook," Aite Group. June 2014

The U.K. payments ecosystem began a transition to EMV chip technology in 2001. In 2005, a liability shift occurred in which the entity with the lowest form of technology (i.e., not EMV-compliant), would be responsible for fraud on a given transaction.

Between the date of the liability shift in 2005, card-not-present fraud increased dramatically, peaking at GBP328 million in 2008, a 79% increase.