

## Cybersecurity



Tasia Hane-Devore  
Staff Writer

Cybersecurity is on the nation's radar, and for good reason: The Center for Strategic and International Studies estimates the cost of cybercrime to the global economy at \$445 billion in a typical year, and Bloomberg projects security spending for cyber threats will top \$40 billion annually by 2017.

As in other sectors, financial institutions are moving with the times to upgrade their technology, but technological advancement comes at a price, as each new technology introduces complexity and system vulnerability. According to the Financial Services

*As attempts to steal consumers' personal and financial information rise, so does the number of bills introduced to put safeguards in place.*

Sector Coordinating Council (FSSCC), most financial firms experience near-daily cyber-attacks. When cyber-attacks are successful, losses can be profound, costing financial institutions millions of dollars per successful breach—and often harming their reputations in the process.

Regardless of against what type of institution or company these cyber-attacks occur, note FSSCC Chairman Russell Fitzgibbons and Vice Chairman Doug Johnson, they are often intended to compromise consumers' financial information.

## Cybersecurity in the financial sector

Title V of the Gramm-Leach-Bliley Act (GLBA) of 1999 requires that financial institutions develop safeguards to ensure the security of consumer records and to protect against anticipated threats to consumers' information. Following GLBA, federal financial regulators including the Board of Governors of the Federal Reserve System issued supervisory guidance delineating expectations and requirements for information security and risk issues in areas such as authentication, continuity planning, payments collection, and vendor management. Federal banking agencies also require that banks, bank holding companies, and their subsidiaries implement a risk-based response program to address breaches to customer information systems.

For at least the past 14 years, then, the financial services sector has what Fitzgibbons and Johnson note is "a robust data protection and examination and enforcement system" in place, one that requires thorough assessments of risks to consumers' information. But it's no longer enough.

Financial institutions have placed cybersecurity among their highest priorities and are working diligently to protect themselves and consumers from cyber-attacks. Addressing concerns presented by Sen. Elizabeth Warren (D-MA) and Rep. Elijah Cummings (D-Baltimore) in their November 2014 letters to 16 large financial institutions, the FSSCC outlines several initiatives to increase cybersecurity and curb the number of financial-sector breaches. These initiatives include security platforms from a number of third-party vendors working on solutions to assimilate and analyze threat information in order to assist financial services companies in combating cyber-attacks.

Also in process today is collaboration between members of the FSSCC and merchant/retailer associations to address cybersecurity threats affecting merchant and financial services industries. The Merchant and Financial Cybersecurity Partnership brings together financial services, retail, government, and other stakeholders to collaborate on public policy in order to increase information sharing among sectors, improve card-security technology, and build and maintain consumer trust.

## Cybersecurity legislation: 2015

As in the private sector, facilitating cybersecurity through enhanced information coordination is a key focus of the White House and the 114th Congress. Barack Obama issued a February 2015 Executive Order—Promoting Private Sector Cybersecurity Information Sharing—to address cyber threats to the economic and national security of the United States.

---

**Financial institutions have placed cybersecurity among their highest priorities and are working diligently to protect themselves and consumers from cyber-attacks.**

---

While not concerned solely with the financial sector, several cybersecurity-related bills impacting banks and banking have been introduced in the 114th Congress.

Some bills are enjoying bipartisan support in their earliest stages. The Cybersecurity Information Sharing Act of 2015 has had the most success to date and, if passed into law, would encourage voluntary sharing of cyber-threat information while protecting individuals' civil liberties.

A sister-bill in the House, the Protecting Cyber Networks Act introduced in late March has since been referred to the full House for consideration. While the two bills offer liability protection to entities who share cybersecurity information voluntarily, two significant differences lie between them. The House bill would prohibit the use of collected data for surveillance purposes. The Senate bill, in contrast, requires information shared by private entities to first go through the Department of Homeland Security.

A related cybersecurity bill originating in the House is the Cyber Privacy Fortification Act of 2015, which seeks to amend the federal criminal code to provide for criminal and civil penalties if a private entity intentionally neglects to notify an individual of a security breach there is reason to believe has resulted in improper access to "sensitive personally identifiable information." The bill would also require the entity to provide prompt notice of the breach to the US Secret Service or the FBI.

These bills mean to incentivize financial-sector cooperation, which some in Congress argue has been lacking. There are numerous reasons a company or financial institution might hesitate to share cyber-attack information, however. Perceived legal risks to sharing such information act as a deterrent, as does providing information of benefit to competitors or of detriment to one's own sales or stock prices. Finally, if there is no mechanism in place to incentivize information sharing—and currently there is not—one's competitors might take advantage of the information provided but not contribute in turn.

These and other bills seek to remove such roadblocks.

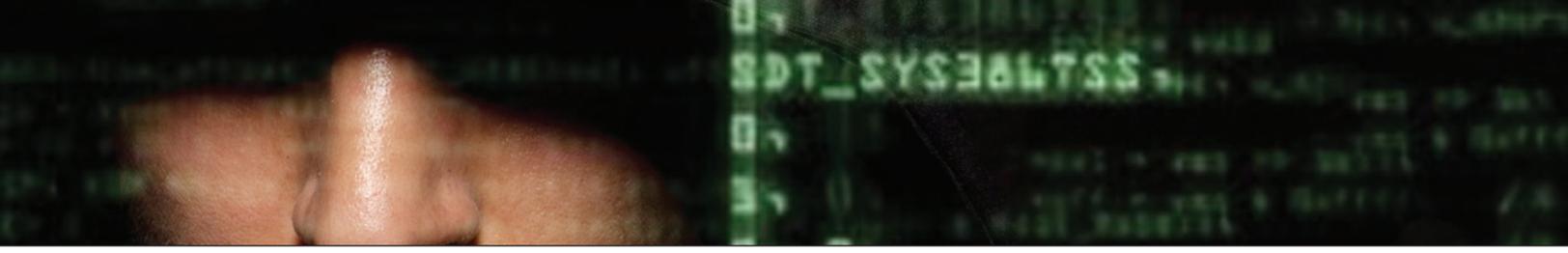
### Cybersecurity and the Federal Reserve

It is, perhaps, out of practicality that the Federal Reserve advocates pursuing non-regulatory and non-legislative approaches in support of cybersecurity strategies whenever possible.

According to the January 2015 report *Strategies for Improving the US Payment System*, there remain important challenges to financial- and retail-sector cybersecurity, "including the time to develop security standards,

## Cybersecurity Legislation Primer

Short title	Cyber Intelligence Sharing and Protection Act (CISPA)	Cyber Privacy Fortification Act of 2015	Cybersecurity Information Sharing Act (CISA) of 2015	Cyber Threat Sharing Act of 2015
Bill Number	H.R. 234	H.R. 104	S. 754	S. 456
Description	An amendment to the National Security Act of 1947 and supported by several trade groups, CISPA would promote information sharing among the government and manufacturing and technology companies.	Reprising a 2013 bill that stalled in committee, H.R. 104 provides for criminal and civil penalties if a private entity neglects to notify consumers of a breach resulting in a loss of "sensitive personally identifiable information."	CISA offers liability protection to companies who share cyber-threat information; a sister-bill, H.R. 1560, is making its way through the House. The Senate version of this bill requires information shared by private companies to first go through the Department of Homeland Security (DHS).	An amendment to the Homeland Security Sharing Act of 2002, this bill would prompt private entities to disclose cyber-threat information to private information-sharing organizations or a federal entity. It would restrict private entities' use and retention of cyber-threat indicators to purposes relating to information security or crime reporting.
Goal	To assist the US government in ensuring network security and investigating cyber threats	To incentivize financial-sector cooperation	To encourage sharing of cyber-threat information while protecting individuals' privacy and civil liberties	To codify mechanisms for enabling cyber-threat information sharing among private entities and between private and government entities
Status (as of press time)	Referred to the House Judiciary and Intelligence Committees	Referred to the House Judiciary Committee	Select Committee on Intelligence; placed on Senate Legislative Calendar No. 28 under General Orders for full Senate consideration	Referred to the Senate Committee on Homeland Security and Governmental Affairs
Follow all bills on <a href="http://www.congress.gov">www.congress.gov</a>	<a href="http://tinyurl.com/lr2z7ob">http://tinyurl.com/lr2z7ob</a>	<a href="http://tinyurl.com/pyqec4s">http://tinyurl.com/pyqec4s</a>	<a href="http://tinyurl.com/q44mcfr">http://tinyurl.com/q44mcfr</a>	<a href="http://tinyurl.com/obwwoh2">http://tinyurl.com/obwwoh2</a>



inconsistent adoption of security improvements, and barriers to sharing fraud and threat information among stakeholders.” Jason Tarnowski, an assistant vice president at the Federal Reserve Bank of Cleveland, observes that technological advances have been embraced by financial institutions, driving innovation in payment and other systems and deepening interconnectedness among financial, retail, utility, and other sectors. “The flip side,” he notes, “is that criminals are exploiting this interconnectedness, presenting significant cybersecurity risks to these firms. Consumers are also at risk, as their bank accounts and personal information are often targeted in these cyber-attacks.”

The Fed’s focus on advancing US payment safety, security, and resiliency reflects an understanding of this interconnectedness—and how vital it is to financial stability. The Strategies report outlines the Fed’s intentions to expand its pool of anti-fraud and risk management services. In the near future, the Fed will explore improvements to its publicly available payment-fraud data, conduct research in payment security, and share results with stakeholders. As a federal banking regulator, the Federal Reserve is strengthening its overall supervisory approach to cybersecurity.

To obtain the current status of bills in the 114th Congress, visit [www.congress.gov](http://www.congress.gov). ■

Data Security Act of 2015	Data Security and Breach Notification Act of 2015	National Cybersecurity Protection Advancement (NCPA) Act of 2015	Personal Data Notification and Protection Act of 2015	Protecting Cyber Networks Act
S. 961	S. 177	H.R. 1731	H.R. 1704	H.R. 1560
Modeled on the data-security and breach-response regime established by the Gramm–Leach–Bliley Act (GLBA) and subsequent guidance issued by financial regulators, including the Federal Reserve Board of Governors, this bill builds on existing law to more effectively ensure information-security procedures are applied consistently. The bill intends to replace the current patchwork of state laws and establish a single set of national standards.	This bill prompts the FTC to broadcast regulations requiring entities that own or process personal information to implement security policies and procedures, including methods for information disposal. It allows an exemption if an institution concludes there is “no reasonable risk of identity theft, fraud, or other unlawful conduct.” Covered entities include those subject to GLBA.	Related to bills H.R. 1560 and S. 754, the NCPA Act would amend the Homeland Security Act of 2002 to enhance civil-liberties protections and multi-directional sharing of cybersecurity information.	Focusing on individual notification rights and responsibilities, this bill requires businesses to notify consumers of breaches to sensitive personally identifiable information. However, if such notification might “cause damage to national security,” notification is not required. Entities excluded from the proposed bill are those that act as vendors of or third-party service providers for vendors of personal health records.	This bill offers liability protection to companies who share cyber-threat information; a sister-bill, S. 754, is making its way through the Senate. Unlike the Senate version, this bill does not require information to first go through DHS. An 11th-hour amendment opposed by many in the financial sector would sunset the standards after 7 years.
To establish a clear set of national standards to prevent and respond to data breaches	To protect consumers’ personal information and to provide for nationwide notice in the event of a security breach	To enhance sharing of information and to strengthen privacy protections	To establish a national data-breach-notification standard	To encourage sharing of cyber-threat information while protecting individuals’ privacy and civil liberties
Referred to the Senate Committee on Commerce, Science, and Transportation	Referred to the House Judiciary and Intelligence Committees	Passed the House 355–63; advanced to the Senate for consideration	Referred to the House Committee on Energy and Commerce and to the Committee on the Judiciary	Passed the House 307–116; advanced to the Senate for consideration
<a href="http://tinyurl.com/knegppj">http://tinyurl.com/knegppj</a>	<a href="http://tinyurl.com/mqyws6r">http://tinyurl.com/mqyws6r</a>	<a href="http://tinyurl.com/k56f76j">http://tinyurl.com/k56f76j</a>	<a href="http://tinyurl.com/nyfdgnj">http://tinyurl.com/nyfdgnj</a>	<a href="http://tinyurl.com/l9ztpcs">http://tinyurl.com/l9ztpcs</a>