5 Takeaways From The New Cybersecurity Executive Order

Law360, New York (October 19, 2014, 9:01 PM ET) --

President Obama signed an executive order on Friday as part of the administration's new BuySecure initiative that requires federal agencies to apply enhanced security features, including chip-and-PIN technology, to government credit cards, debit cards and other payment cards.[1] According to an accompanying fact sheet,[2] the initiative on whole purports to "provide consumers with more tools to secure their financial future by assisting victims of identity theft, improving the Government's payment security as a customer and a provider, and accelerating the transition to stronger security technologies and the development of next-generation payment security tools."

Specifically, the executive order and accompanying fact sheet:

- Require implementation of chip-and-PIN technology to new and existing government credit and debit cards;

- Highlight a variety of steps the private sector has or soon will take in an effort to improve the security of consumer data and protect against credit card fraud and identity theft, including the provision to consumers of regular access to their credit scores and installation of chip-and-PIN point of sale terminals;

- Outline a number of credit score transparency and identity theft prevention measures, including steps to make credit scores more widely available and an expansion of existing information sharing efforts to strengthen federal law investigators' ability to report evidence of stolen information to companies with affected consumers;

- Announce a cybersecurity and consumer protection summit involving key stakeholders to be held later this year; and

- Call upon Congress to enact data breach and cybersecurity legislation.

As cyberattacks against participants in the financial system have become more frequent, sophisticated and pervasive, financial institutions, retail businesses and payment processors of all sizes and types are integrating cyber-risk into their governance, risk management and information technology systems, devoting significant resources to confronting a problem that is not likely to soon dissipate. The president's executive order and BuySecure initiative augment the administration's existing efforts to improve cybersecurity in ways that merit consideration by these market participants.

First, the executive order encourages prompt cybersecurity measures in an effort to protect consumer data in connection with credit card, debit card and retail payment transactions. The

executive order commits the government to transition payment processing terminals and credit, debit and other payment cards to use enhanced security features, including chip-and-PIN technology, taking into consideration relevant voluntary consensus standards. The government will take the steps necessary to ensure that acquired payment processing terminals have enhanced security features no later than Jan. 1, 2015, and to develop a plan for federal agencies to install enabling software by the same date. Additionally, the Direct Express prepaid debit card program through which the government provides electronic Social Security and Supplemental Security income, Veterans Administration and other payments will have enhanced security features by the same date.

Government use of chip-and-PIN technology is a key element of the executive order and is characterized in the fact sheet as a way to help drive the market forward toward more secure payment systems. Chip-and-PIN or EMV chip cards contain embedded microprocessors that provide transaction security at a level that is not possible with traditional magnetic strip cards. Many consumers already have EMV chip technology on their credit cards and thus have greater protection against fraudulent transactions in face-to-face transactions.

Second, the executive order highlights the importance of improving the process and timeliness of remediating identity theft. The government will take steps to assist victims of identity theft by supporting the development of a new one-stop resource at the Federal Trade Commission's IdentityTheft.gov that is intended to help consumers with remediation efforts. Since the goal is to build a more accessible portal through which reports of fraud can be submitted to multiple credit reporting bureaus, the government will partner with the credit reporting bureaus to improve the foundation of IdentityTheft.gov. The government intends to make the enhanced site available to the public by May 15, 2015.

Additionally, the executive order expands information-sharing among federal agencies to try to reduce the average amount of time required for a consumer to remediate identity theft. In this regard, the attorney general, in coordination with the secretary of Homeland Security, must issue guidance to promote regular submissions by federal law enforcement agencies of compromised credentials to the National Cyber-Forensics and Training Alliance's Internet Fraud Alert System, as permitted by law.

Third, the executive order recognizes that no single technology provides complete information security protection. A plan is required to be presented to the president, within 90 days, to ensure that all federal agencies that make consumer data accessible to citizens through digital applications require multiple layers of authentication, and that relevant agencies carry out such plan within 18 months.

Fourth, the fact sheet encourages private sector participants to offer more secure options to their customers. The fact sheet and the president's remarks before the Consumer Financial Protection Bureau commend private sector actions to improve the security of consumer financial transactions.[3] Notable examples include financial institutions that provide consumers' regular access to their credit scores to assist in the detection of fraud and that assist small business customers in upgrading their point-of-sale terminals, retailers that install chip-and-PIN point of

sale terminals, and organizations that educate consumers and merchants on the use of secure technologies.

Fifth, the fact sheet calls for Congress to enact cybersecurity legislation. According to the fact sheet, legislation would help the government protect federal networks and would clarify the actions companies must take regarding notification to their customers following security breaches. Additionally, in his remarks to the CFPB, the president stated, "Today, data breaches are handled by dozens of separate state laws, and it's time to have one clear national standard that brings certainty to businesses and keeps consumers safe."

The administration views chip-and-PIN technology as a significant step forward, but such technology does not provide protection in online, mail and telephone order purchases, and does not eliminate the risk of a security breach. Accordingly, financial institutions and merchants should view use of this technology not as a panacea for payment card security but rather as one component of a sound cybersecurity position. Financial institutions and merchants additionally should consider participating in public-private coalitions to develop and maintain best practices. And they should review the administration's cybersecurity framework, issued in February 2014 by the National Institute of Standards and Technology, to assess whether its adoption would be appropriate.[4]

Cybersecurity is a topic worthy of increased attention. In the present regulatory environment, financial institutions and merchants alike should consider the security of consumer financial transactions — and the mitigation of associated legal liabilities — as a high priority.

—By Lisa Ledbetter, Mauricio Paez, Michael Butowsky and Jay Johnson, Jones Day

Lisa Ledbetter is a partner in Jones Day's Washington, D.C., office. Mauricio Paez and Michael Butowsky are partners in the firm's New York office. Jay Johnson is of counsel in the firm's Dallas office.

[1] The executive order, titled Improving the Security of Consumer Financial Transactions, is available at http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions.

[2] The fact sheet accompanying the executive order is available at http://www.whitehouse.gov/the-press-office/2014/10/17/fact-sheet-safeguarding-consumers-financial-security.

[3] The president's remarks before the CFPB are available at http://www.c-span.org/video/?322175-1/president-obama-consumer-financial-security.

[4] The administration's cybersecurity framework is available at http://www.nist.gov/cybersecurity-framework-021214-final.pdf.