Cooley

October 28, 2014

On Friday, October 17, Obama signed his second major cyber-related executive order in the past two years. This most recent EO, entitled "Improving the Security of Consumer Financial Transactions," focuses squarely on the massive data breaches that continue to plague numerous companies. In fact, the Fact Sheet from the White House stated a need to act resulting from "over 100 million Americans falling victim to data breaches over the last year, and millions suffering from credit card fraud and identity crimes." To realize improvements, the administration will utilize mechanisms within its power to make changes to the way government does business.

Using a combination of policy initiatives related to both payment technologies and identity theft remediation, Obama wants "all stakeholders to join the Administration and a number of major corporations in driving the economy toward more secure standards to safeguard consumer finances." One goal is to improve security by "employ[ing] enhanced security features." In particular, the Administration will move toward using only payment systems and technologies that are believed to contain higher levels of security than those systems in use today.

Section 1 of the EO describes how executive departments and agencies will transition from traditional magnetic stripe terminals and payment cards to newer chip-and-PIN technology. Based on older technology known as EMV (Europay-Mastercard-Visa), chip-and-PIN comprises a computer chip on the payment card or smart card that securely (using cryptographic techniques) communicates with the reader, thereby securing the sensitive credit card information. The EO directs GSA and Treasury to "take necessary steps to ensure that…payment cards provided through [GSA] contracts have these and other enhanced security features." Other agencies that utilize payment cards must develop transition plans as well.

Section 2 of the EO seeks to improve the ability of consumers to remediate incidents of identity theft. The Administration directs numerous agencies to be involved in these efforts. DHS will issue guidance regarding the reporting of compromised credit cards to a national cyber-forensics clearinghouse. DOJ, Commerce, and SSA will provide information to the FTC on publicly available resources for handling identity theft. Finally, OMB and GSA will help the FTC enhance the functionality of IdentityTheft.gov.

All of this follows on Executive Order 13636. Signed in February 2013 by President Obama, EO 13636 is entitled "Improving Critical Infrastructure Cybersecurity." Reportedly fed up with Congress' inability to move forward on improving the cyber posture in the U.S., EO 13636 laid out a cyber agenda that included a mandate that led to the NIST Framework. One interesting thing about the 2013 EO is the reception to it by the business public. A recent Deloitte-NASCIO study showed the almost 30% of state CISOs plan to adopt the NIST Framework in the next year. This could have the same effect on the private sector that the new EO is intended to have (i.e., the private sector winds up inevitably following what the government is doing).

One of the most remarkable things about the new EO is that all of the activity described above is scheduled to be completed by January 1, 2015. That's less than three months away. Clearly, many of the efforts had to have been underway before the EO was signed. While the various activities will arguably increase certain aspects of the security in the system, all stakeholders will need to continue to be vigilant in other areas of security in order to stay ahead of the cyber attackers. For companies that deal with credit card transactions, the new EO should be seen as a turning point in electronic transactions and those companies should be prepared for the new chip-and-PIN.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090