Executive Order 13681—Improving the Security of Consumer Financial Transactions

October 17, 2014

Given that identity crimes, including credit, debit, and other payment card fraud, continue to be a risk to U.S. economic activity, and given the economic consequences of data breaches, the United States must take further action to enhance the security of data in the financial marketplace. While the U.S. Government's credit, debit, and other payment card programs already include protections against fraud, the Government must further strengthen the security of consumer data and encourage the adoption of enhanced safeguards nationwide in a manner that protects privacy and confidentiality while maintaining an efficient and innovative financial system.

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to improve the security of consumer financial transactions in both the private and public sectors, it is hereby ordered as follows:

Section 1. Secure Government Payments. In order to strengthen data security and thereby better protect citizens doing business with the Government, executive departments and agencies (agencies) shall, as soon as possible, transition payment processing terminals and credit, debit, and other payment cards to employ enhanced security features, including chip-and-PIN technology. In determining enhanced security features to employ, agencies shall consider relevant voluntary consensus standards and specifications, as appropriate, consistent with the National Technology Transfer and Advancement Act of 1995 and Office of Management and Budget Circular A–119.

(a) The Secretary of the Treasury shall take necessary steps to ensure that payment processing terminals acquired by agencies through the Department of the Treasury or through alternative means authorized by the Department of the Treasury have enhanced security features. No later than January 1, 2015, all new payment processing terminals acquired in these ways shall include hardware necessary to support such enhanced security features. By January 1, 2015, the Department of the Treasury shall develop a plan for agencies to install enabling software that supports enhanced security features.

(b) The Administrator of General Services shall take necessary steps to ensure that credit, debit, and other payment cards provided through General Services Administration (GSA) contracts have enhanced security features, and shall begin replacing credit, debit, and other payment cards without enhanced security features no later than January 1, 2015.

(c) The Secretary of the Treasury shall take necessary steps to ensure that Direct Express prepaid debit cards for administering Government benefits have enhanced security features, and by January 1, 2015, the Department of the Treasury shall develop a plan for the replacement of Direct Express prepaid debit cards without enhanced security features.

(d) By January 1, 2015, other agencies with credit, debit, and other payment card programs shall provide to the Office of Management and Budget (OMB) plans for ensuring that their credit, debit, and other payment cards have enhanced security features.

(e) Nothing in this order shall be construed to preclude agencies from adopting additional standards or upgrading to more effective technology and standards to improve the security of consumer financial transactions as technologies and threats evolve.

Sec. 2. Improved Identity Theft Remediation. To reduce the burden on consumers who have been victims of identity theft, including by substantially reducing the amount of time necessary for a consumer to remediate typical incidents:

(a) by February 15, 2015, the Attorney General, in coordination with the Secretary of Homeland Security, shall issue guidance to promote regular submissions, as appropriate and permitted by law, by Federal law enforcement agencies of compromised credentials to the National Cyber-Forensics and Training Alliance's Internet Fraud Alert System;

(b) the Department of Justice, the Department of Commerce, and the Social Security Administration shall identify all publicly available agency resources for victims of identity theft, and shall provide to the Federal Trade Commission (FTC) information about such resources no later than March 15, 2015, with updates thereafter as necessary. These agencies shall work in consultation with the FTC to streamline these resources and consolidate them wherever possible at the FTC's public website, IdentityTheft.gov; and

(c) OMB and GSA shall assist the FTC in enhancing the functionality of IdentityTheft.gov, including by coordinating with the credit bureaus to streamline the reporting and remediation process with credit bureaus' systems to the extent feasible, and in making the enhanced site available to the public by May 15, 2015.

Sec. 3. Securing Federal Transactions Online. To help ensure that sensitive data are shared only with the appropriate person or people, within 90 days of the date of this order, the National Security Council staff, the Office of Science and Technology Policy, and OMB shall present to the President a plan, consistent with the guidance set forth in the 2011 National Strategy for Trusted Identities in Cyberspace, to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate. Within 18 months of the date of this order, relevant agencies shall complete any required implementation steps set forth in the plan prepared pursuant to this section.

Sec. 4. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(b) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

The White House,
October 17, 2014.

[Filed with the Office of the Federal Register, 11:15 a.m., October 22, 2014]

NOTE: This Executive order was published in the *Federal Register* on October 23.

Categories: Executive Orders : Consumer financial transactions, improving security.

Subjects: Business and industry : Consumer data security, strengthening efforts; Government organization and employees : Consumer financial transactions and data security, strengthening efforts.

DCPD Number: DCPD201400778.