Client Update
U.S. Authorizes Cyber Sanctions, Recommends Tech Companies Adopt Compliance Programs

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Carl Micarelli
cmicarelli@debevoise.com

James J. Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.
Satish M. Kini
smkini@debevoise.com

David A. O'Neil
daoneil@debevoise.com

Robert T. Dura
rdura@debevoise.com

Veronica R. Glick
vrglick@debevoise.com

On April 1, 2015, President Obama issued Executive Order (E.O.) 13694, authorizing new blocking sanctions (asset freezes) against persons that engage in certain significant and malicious cyber-enabled activities that threaten the United States.

Pursuant to the Executive Order, the Treasury Secretary, in consultation with the U.S. Attorney General and the Secretary of State, may impose sanctions on any individual or entity that engages in cyber-enabled activities "originating from, or directed by persons located, in whole or in substantial part, outside the United States" that cause, or seek to cause, significant harm or disruption to computers, computer networks or any of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21 (*i.e.*, the 2013 directive on Critical Infrastructure Security and Resilience). Additionally, E.O. 13694 authorizes sanctions against persons that steal significant funds, trade secrets or other personal or financial information, as well as those that knowingly receive or make use such stolen information.

No persons have yet been designated under the Executive Order, but those designated will be added to the Office of Foreign Assets Control's ("OFAC") list of Specially Designated Nationals and Blocked Persons. In the meantime, and concurrent with the issuance of the Executive Order, OFAC issued a list of Frequently Asked Questions ("FAQs").

In those FAQs, OFAC reminds U.S. persons (and persons otherwise subject to OFAC jurisdiction) that they must ensure they are not engaging in transactions with any persons named under the Executive Order. To this end, OFAC specifically calls on "firms that facilitate or engage in online commerce" and other technology companies to develop "a tailored, risk-based compliance

program, which may include sanctions list screening or other appropriate measures."

Until now, the U.S. government has focused principally on the need for banks and other financial services companies to have robust sanctions programs. This FAQ appears to be the first time that U.S. authorities have expressly voiced an expectation that technology companies should develop and implement sanctions-specific compliance regimes. It may be prudent for technology companies to review their sanctions-related risks and consider enhancing their compliance programs accordingly.

For technology and e-commerce companies, designing and implementing a risk-based sanctions compliance program – or enhancing an existing program – may present unique challenges. Many such companies have global user bases and operate under business models in which they may not readily be able to identify and verify the identity of customers, independent contractors, users and other counterparties prior to the provision of services. OFAC's recent $7.7 million settlement with PayPal, Inc. ("PayPal") highlights the importance of designing and implementing effective sanctions compliance programs. The settlement agreement suggests PayPal failed to maintain adequate sanctions screening and monitoring procedures and consequently processed transactions in apparent violation of U.S. sanctions related to Cuba, Iran, Sudan, global terrorism and the nonproliferation of weapons of mass destruction.

E.O. 13694 is the latest development in the U.S. government's use of sanctions to deter and punish global cyber-crimes. Earlier this year, President Obama issued E.O. 13687, authorizing expanded sanctions on North Korea's government in response to the cyber-attack on Sony Pictures Entertainment, among other provocations. In December, Section 1637 of the National Defense Authorization Act for fiscal year 2015 authorized the President to impose blocking sanctions on any non-U.S. person determined to knowingly support, facilitate or benefit from the "significant appropriation," through espionage in cyberspace, of U.S. technologies or proprietary information. Pub. L. No. 113-291, 128 Stat. 3292.

For a semi-monthly e-mail summary of developments in economic and trade sanctions, please subscribe to the Debevoise & Plimpton LLP Sanctions Alert. To subscribe, please e-mail sanctions@debevoise.com or sign up here. The Firm's sanctions-related publications may also be found at The Sanctions Resource.

* * *

Please do not hesitate to contact us with any questions.