April 2015

Regulatory brief

A publication of PwC's financial services regulatory practice

Sanctions: US action on cyber crime

Overview

On April 1st, President Obama issued an Executive Order ("EO") establishing the first-ever economic sanctions program in response to cyber attacks. The EO will impact individuals and entities ("designees") responsible for cyber attacks that threaten the national security, foreign policy, economic health, or financial stability of the US.

Specifically, the EO authorizes the Treasury Department to freeze designees' assets. Although none have yet been named, we believe the EO was issued with specific designees in mind and expect designations to follow shortly.[1] Given the EO's broad scope that covers "entities" (including foreign governments and their affiliates), it may also be used to help deter state-sponsored cyber crimes.

Once designees are announced, financial institutions should take steps to ensure they do not engage in prohibited dealings with them. In addition, institutions that are targeted by cyber criminals will see an increase in government inquiries to assist in building cases against potential targets of sanctions.

Background and detail

The EO comes in the wake of recent cyber attacks on major US businesses and financial institutions including:

- Anthem (February 2015): Hackers stole confidential information on millions of customer and employees, including Social Security numbers, birth dates, and addresses
- Sony Pictures (November 2014): Alleged North Korean hackers accessed (and subsequently released) the company's emails, contracts, and confidential employee information
- JPMorgan Chase (July 2014): Hackers made off with millions of customers' basic identifying information (names, addresses, telephone numbers, and emails)
- Target (December 2013): One of the largest cyber attacks in history that resulted in the loss of credit and debit card information, as well as customers' names, addresses, and emails

[1] The names will then be added to the Office of Foreign Assets Control's ("OFAC") Specially Designated Nationals ("SDN") and Blocked Persons lists.

pwc

In this first US categorical response, the EO authorizes the following types of persons and entities to be designated for asset freezes:

- Any who carry out cyber attacks that are originated or directed from outside of the US, and are likely to threaten the US
- Any who receive or use trade secrets misappropriated via cyber attacks
- Any who materially assist in either of these activities

As a consequence, US individuals or entities, wherever located, will be prohibited from any dealings with these designees that involve their property or property interests. Exchanging funds, goods, or services will also be prohibited (including making or receiving donations).

Going forward, financial institutions should add designees to their screening filters and review their existing accounts and relationships.[2] Globally active firms should also monitor developments in other jurisdictions, especially the EU, which we expect will introduce similar programs.

[2] See PwC's *Regulatory brief*, *Sanctions: US and EU action on Ukraine* (March 2014) for more detail.

Additional information

For additional information about this **Regulatory brief** or PwC's Financial Services Regulatory Practice, please contact:

Dan Ryan
Financial Services Advisory Leader
646 471 8488
daniel.ryan@us.pwc.com

Mike Alix
Financial Services Advisory Risk Leader
646 471 3724
michael.alix@us.pwc.com

Adam Gilbert
Financial Services Global Regulatory Leader
646 471 5806
adam.gilbert@us.pwc.com

Armen Meyer
Director of Regulatory Strategy
646 531 4519
armen.meyer@us.pwc.com

Contributors: Daniel Tannebaum, Amber Stokes, John Engler, Melissa Jameson, and Gregory Schwarz.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs