KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group
International Trade & Litigation Practice Group

January 13, 2016

OFAC Codifies Cyber-Related Sanctions Regulations But Questions Remain

On December 31, 2015, the Treasury Department's Office of Foreign Assets Control (OFAC) issued **new regulations** that codify the U.S. Cyber-Related Sanctions program. These regulations (31 C.F.R. Part 578) implement President Obama's **Executive Order 13694** entitled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activity" issued on April 1, 2015. While the OFAC codification is a necessary step in implementing the cyber-related sanctions, OFAC's regulations leave many unanswered questions about how and when OFAC will exercise its authority in practice, which will be answered in supplemental regulations.

As King & Spalding **previously reported**, EO 13694 is a broad and flexible tool authorizing sanctions on individuals or entities that are responsible for, complicit in, or engage in malicious cyber-enabled activities originating or directed from abroad. The cyber-enabled activities must significantly threaten the national security, foreign policy, or economic health or financial stability of the United States. In addition, the activities must have the purpose or effect of

- Harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
- Significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
- Causing significant disruption to the availability of a computer or network of computers; or
- Causing significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

Furthermore, the EO authorizes sanctions against those who knowingly receive or benefit from trade secrets misappropriated through cyber-enabled means for commercial or competitive advantage or private financial gain.

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Christine E. Savage
+1 202 626 5541
csavage@kslaw.com

Jeffrey M. Telep
+1 202 626 2390
jtelep@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

Nicholas A. Oldham
+1 202 626 3740
noldham@kslaw.com

Kerianne Tobitsch
+1 212 556 2310
ktobitsch@kslaw.com

Elizabeth E. Owerbach
+1 202 626 9223
eowerbach@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

Key Features of the OFAC Regulations

The OFAC regulations became effective on December 31, 2015. Moreover, because the regulations "involve a foreign affairs function," OFAC published the regulations as a Final Rule after concluding that notice and comment rulemaking procedures were not required. OFAC has stated its intent to supplement this Final Rule "with a more comprehensive set of regulations." These future amendments will likely be implemented in the same way, leaving individuals and companies little time to adjust.

As published, the OFAC regulations present a standard "blocking" program, similar to other programs in which parties are placed on OFAC's **Specially Designated Nationals** (SDN) list. Although no entities or individuals have yet been designated under the EO or OFAC's regulations, entities designated under the cyber-related sanctions program will be added to the SDN list, tagged with the identifier "[CYBER]," or "[BPI–CYBER]," which means the entities are blocked during the pendency of an investigation.

The U.S. will block the property and interests in property of any designated entities, meaning that all property and interests in property that are in the United States, that come within the United States, or that come within the possession or control of any United States person may not be transferred, paid, exported, withdrawn, or otherwise dealt in. These sanctions will also follow the OFAC "50 percent rule," meaning that for any entity in which blocked parties have, individually or in the aggregate, directly or indirectly, a 50 percent or greater interest in that entity, that entity itself becomes blocked. The regulations render any transfer involving blocked property or interests in property null and void. Generally, U.S. persons in possession of funds subject to the blocking order must hold or place such blocked funds in an interest-bearing account located in the United States.

As with other sanctions regimes overseen by OFAC, the new regulations include standard provisions that permit (i) designated entities to obtain legal advice provided that the receipt of payment for professional fees is "specifically licensed" as well as emergency medical services "in the United States" and (ii) financial institutions to hold blocked assets in interest bearing accounts for investment and reinvestment purposes and to debit normal service charges.

Finally, the OFAC regulations include a formal delegation of authority from the Secretary of Treasury to the "Director of OFAC or [] any other person to whom the Secretary of the Treasury has delegated authority" to act under the EO, which will expedite future designations.

Unanswered Questions Remain—Additional OFAC Action Is Likely

As published, the OFAC regulations essentially serve as a framework for future designations but shed little insight into exactly how OFAC will exercise its expansive authority to designate individuals or entities for "cyber-enabled" activities. And as of the date of this publication, OFAC has not yet designated any parties under this sanctions program. Indeed, OFAC itself signed its intention to "supplement" these framework regulations "with a more comprehensive set of regulations" that "may include additional interpretive and definitional guidance and additional general licenses and statements of licensing policy." It is not clear when OFAC will issue this interpretive or definitional guidance.

Similarly, the precise definition of what constitutes a "cyber-enabled" activity remains unclear. OFAC has indicated that it may provide a definition of "cyber-enabled" activities when it issues its supplemental regulations, but in the meantime how OFAC interprets "cyber-enabled" activity will greatly impact the reach of these regulations. OFAC **hinted** in April that "malicious cyber-enabled activities include deliberate activities accomplished through

unauthorized access to a computer system, including by remote access; circumventing one or more protection measures, including by bypassing a firewall; or compromising the security of hardware or software in the supply chain." This description of what could constitute "cyber-enabled" activity is quite broad and could potentially cover a wide range of cybersecurity incidents. How OFAC plans to exercise its sanctions authority or otherwise narrow this definition is unknown at this time. Finally, how these terms are defined in practice and how OFAC exercises its designation authority may clarify some of these questions in the future. For example, will OFAC act on its own to designate individuals or entities for cyber-related activities or will OFAC designations in this area be rolled out as part of a broader and more comprehensive U.S. Government response to rogue individuals and regimes.

As OFAC acting director John Smith has **stated**, the cyber-related sanctions program will enable the United States to target illicit foreign cyber activity "wherever it arises" and is "intended to counter the most significant cyber threats" faced by the United States. OFAC likewise stated that "compromise to critical infrastructure, denial of service attacks, or massive loss of sensitive information, such as trade secrets and personal financial information" accomplished through or facilitated by computers or electronic devices could qualify under the EO and therefore OFAC's regulations. After the June 2015 announcement by the Office of Personnel Management that it has been the target of a data breach targeting the records and sensitive personal information of millions of current and former federal employees, many had speculated that the sanctions would be used to target Chinese entities, but the administration has thus far refrained from doing so.

Another key question will be how OFAC will attribute cyber activities to particular individuals or entities as part of the designation process. How individuals will be given an opportunity to review and challenge the information that purports to attribute cyber activities to them will raise numerous questions that could take years to work out given the highly technical nature of attribution of computer incidents.

However OFAC answers these questions in future amendments to its regulations, it is clear that such amendments or modifications will not affect OFAC's actions under its regulations, and all "penalties, forfeitures, and liabilities" will continue and may be enforced as if such amendments or modifications had not been made.

Recommendations

As OFAC's recent rulemaking shows, the U.S. Government continues to focus on cybersecurity risks and means to counter malicious cyber activity. Moreover, the rulemaking once again demonstrates how cyber incidents may swiftly escalate to business crises, and may create legal predicaments. As a result, companies should assess potential threats to information systems and find cost-effective means to reduce the likelihood of incidents and minimize the business and legal impact of such incidents. For example, companies should have a compliance program to monitor and abide by OFAC's designations and seek licenses as necessary to cover their activities.

King & Spalding will continue to monitor developments with regard to this sanctions program and will provide updates if new regulations or guidelines are implemented or if individuals are designated under this program. We invite you to consult with us further regarding the implications of this new authority.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our **Data, Privacy & Security Practice** regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation

arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 60 Data, Privacy & Security lawyers in offices across the United States, Europe, Russia, and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and data security-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

King & Spalding's International Trade/WTO Practice

King & Spalding's **International Trade Group**, headquartered in the Washington, D.C., and Geneva offices, handles a wide range of international trade matters for U.S. and non-U.S. clients. The group's export controls and sanctions practice provides assistance to clients on compliance with U.S., U.K., and EU law and regulations. Our main goal is to help clients achieve their business objectives in compliance with this constantly changing area of the law. Lawyers in the group assist clients in navigating all stages of government regulation, including assisting with sanctions compliance, export classification and licensing, developing and implementing internal compliance systems, investigating violations, and responding to enforcement actions brought by government trade control agencies.