KING & SPALDING

Client Alert

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

November 1, 2016

FinCEN Issues Advisory on Cyber Crime

On October 25, the U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") published an Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime and an accompanying Frequently Asked Questions document. The Advisory aims to assist financial institutions in understanding their Bank Secrecy Act ("BSA") obligations regarding cyber-events and cyber-enabled crime. While the advisory does not change any existing regulatory requirements, it offers guidance for financial institutions to better understand how to identify, report, and share information under the BSA.

Reporting on Cyber-Events

In the Advisory, FinCEN defines a "cyber-event" as "an attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information." Cyber-events may trigger mandatory or voluntary reporting of Suspicious Activity Reports ("SARs").

Mandatory Reporting

Mandatory reporting is required for a suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets. The Advisory offers the following guidance for determining whether a cyber-event has triggered mandatory reporting:

- Cyber-events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities.
- Financial institutions should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted.
- To determine monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event.

For more information, contact:

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

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

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

Betere M. Gizaw
+1 202 626 8974
bgizaw@kslaw.com

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

King & Spalding
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

- Financial institutions should consider any other cyber-related SAR filing obligations required by functional regulators, such as the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA).

Voluntary Reporting

FinCEN encourages financial institutions to report egregious, significant, or damaging cyber-events and cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR. For instance, if a financial institution determines that a Distributed Denial of Service attack has disrupted a financial institution's website and disabled the institution's online banking services for a significant period of time, it should consider reporting it even if the institution determines that the attack was not intended to and could not have affected any transactions.

Information to Include in an SAR filing

When filing either a mandatory or voluntary SAR, financial institutions are encouraged to include:

- Description and magnitude of the event
- Known or suspected time, location, and characteristics or signatures of the event
- Indicators of compromise
- Relevant IP addresses and their timestamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant.

Collaboration between BSA and Anti-Money Laundering ("AML") and Cybersecurity Units

The Advisory stresses the importance of financial institutions collaborating internally with BSA/AML staff, cybersecurity personnel, fraud prevention teams, and other units potentially affected by a cyber-event. Cooperation will enable firms to better assess, analyze, and report on suspicious cyber activity.

Sharing Cyber-Related Information between Financial Institutions

FinCEN encourages financial institutions to share pertinent cyber-related information among one another, noting that information about specific malware signatures, IP addresses and device identifiers, and seemingly anonymous virtual currency addresses may be helpful in identifying cyber criminals. Financial institutions are encouraged to take advantage of the safe harbor provisions of Section 314(b) of the USA PATRIOT Act which enable institutions to share cyber-related information regarding individuals, entities, organizations, and countries for the purposes of identifying and reporting money laundering and terrorist activities. Failure to comply with the safe harbor requirements will result in the loss of the safe harbor protection for information sharing and may result in a violation of privacy laws or other laws and regulations. Further, financial institutions should take precautions to protect attorney-client communications and attorney work product when sharing cyber related information.

U.S. financial institutions are attractive targets for cyber criminals, and financial institutions are encouraged to implement the guidelines in the Advisory. King and Spalding will continue to monitor FinCEN for further updates and guidance.

King & Spalding's Data, Privacy & Security Practice

With more than 60 Data, Privacy & Security lawyers in offices across the United States, Europe, 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 cybersecurity-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. Our Data, Privacy & Security Practice has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.