EVERSHEDS SUTHERLAND

Horizon scanner
Financial Crime – US

RISK RATING

Potential impact

Legal issue/risk	When?	What's next	Supporting information
The US Department of Justice revised the Evaluation of Corporate Compliance Programs guidance. The Evaluation of Corporate Compliance Programs provides guidance to prosecutors conducting an investigation of a corporation and determining whether to bring charges. Since 2017, the guidance has undergone several revisions intended to provide clarity and transparency. The June 2020 revisions provide useful insight into the US Department of Justice's current focus, which includes (i) the ongoing evolution of a company's compliance program; (ii) the need to evaluate the compliance program based on a company's individual circumstances; (iii) the importance of ensuring the compliance function is sufficiently resourced and has appropriate authority; and (iv) the compliance function's access to and use of data to accomplish these goals.	1 June 2020	Companies should evaluate their compliance programs to ensure they are adequate, particularly in areas related to ongoing testing and review of the compliance program, the program's ability to address evolving and emerging risks, the resources and information available to the compliance function, and whether personnel are able to implement the compliance program effectively.	US Department of Justice Evaluation of Corporate Compliance Programs "US Department of Justice revises DOJ Corporate Compliance Program evaluation guidelines"
The US Supreme Court limited the US Securities and Exchange Commission's authority to seek disgorgement. In June 2020, the US Supreme Court rendered its decision in Liu v. SEC, a case that challenged the SEC's authority to obtain disgorgement. The Supreme Court upheld the SEC's ability to seek disgorgement, but imposed limitations on how disgorgement is calculated and how collected funds are used. Historically, the SEC could order disgorgement of a wrongdoer's ill-gotten proceeds. The Liu decision limits disgorgement to net profits and requires deduction of legitimate business expenses from the amount of the ill-gotten gains. The decision also held that the SEC cannot impose joint-and-several liability for disgorgement unless	22 June 2020	How the SEC will apply these principles in practice is uncertain, and there inevitably will be additional litigation to define those limitations. In the meantime, companies in settlement discussions with the SEC should consider how they can use the Liu decision to their advantage. Companies may be able to obtain significantly reduced penalties if they can show that the net profits from the alleged wrongdoing were less than the alleged ill-gotten proceeds. Companies may also be able to	Liu v. SEC decision

 Immediate impact

 Short-term impact

 On the horizon

Legal issue/risk	When?	What's next	Supporting information
it can show that the wrongdoers engaged in "concerted wrongdoing". The Supreme Court held that disgorgement must be "for the benefit of investors". The funds collected from the disgorgement must be returned to the victims or otherwise be used for the victims' benefit.		argue that any disgorgement is inappropriate if the SEC cannot identify harmed investors that could benefit from the disgorgement.	
FinCEN issued an Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic. On 30 July 2020, the Financial Crimes Enforcement Network (FinCEN) released the "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," which explains how cybercriminals are using the COVID-19 pandemic to their advantage, capitalizing on remote access and exploiting financial institutions, businesses, and their customers to commit fraud, identity theft and generally disrupt business. According to the Advisory, FinCEN has observed an increase in cybercriminals (i) targeting and exploiting the use of remote platforms and processes; (ii) engaging in phishing, malware and extortion; and (iii) using business email compromise schemes to commit fraud and interrupt business and supply chains. The Advisory describes "red flags" under each category—twenty potential indicators of cybercrime in total—used most often by criminals to exploit vulnerabilities created or exacerbated by the COVID-19 pandemic.	30 July 2020	FinCEN is focused on whether financial institutions have systems in place to effectively mitigate the risks that cybercriminals pose to financial institutions and their customers, and the Advisory is likely a preview of future enforcement trends. Financial institutions should assess their systems proactively to determine if their current framework adequately addresses cybercrime risks that put them and/or their customers in harm's way.	FinCEN Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic "FinCEN advisory highlights increased cybercrime risks during COVID-19"
The US Department of Commerce's Bureau of Industry and Security amended the foreign-produced direct product rule targeting Huawei. On May 15, 2020, the US Department of Commerce's Bureau of Industry and Security (BIS) expanded its	17 August 2020	Global companies that export products to, or otherwise engage in business with, Huawei or its affiliates should consider the implications of the	Department of Commerce Final Rule: Addition of Huawei Non-U.S. Affiliates to the

Immediate impact Short-term impact On the horizon

Legal issue/risk	When?	What's next	Supporting information
export controls on Huawei Technologies Co. Ltd. (Huawei) by amending the foreign-produced direct product rule, which became final on 17 August. BIS originally placed Huawei, the Chinese telecommunications giant, and 68 of its non-US affiliates on the Entity List on May 21, 2019 (effective May 16, 2019), and later added 46 additional non-US affiliates of Huawei to the Entity List on August 21, 2019 (effective August 19, 2019). Placement on the Entity List effectively prohibits the sale, export or transfer of US-origin products, technology or software (items that are subject the Export Administration Regulations (EAR)), to Huawei and its affiliates without a license from BIS. There is a presumption of denial licensing policy for Huawei and its affiliates, making it unlikely that a license request will be granted. The newly amended "foreign-produced direct product" rule, as it applies to Huawei and its affiliates on the Entity List, provides that even if items are produced outside of the US, these items may still be subject to the EAR if: (i) the item contains a certain controlled US-origin content; or (ii) the item is the direct product of certain US-origin technology or software. The amendment also expands the types of US-origin technology and software for which a foreign-produced item is considered to be a direct product. The amendment effectively restricts Huawei's ability to acquire semiconductors and chipsets produced outside the US with the help of equipment that has been produced from US software and technology.		new amendment on these activities. It will be additionally critical for business to stay apprised of any further US restrictions on Huawei.	Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)
FinCEN issued a Statement on Enforcement of the Bank Secrecy Act. On 18 August 2020, FinCEN issued a statement reviewing its statutory authority to enforce the Bank Secrecy Act	18 August 2020	While the statement does not contain any groundbreaking information, it may signal increased BSA enforcement in the near future. Companies	FinCEN Statement on Enforcement of the Bank Secrecy Act


Immediate impact


Short-term impact


On the horizon

Legal issue/risk	When?	What's next	Supporting information
(BSA). The statement sets forth FinCEN's six different enforcement "approaches" to BSA violations, such as issuing no action or warning letters, imposing civil monetary penalties and making criminal referrals. It also lists factors that FinCEN will consider when determining appropriate sanctions. These factors include self-disclosure, cooperation, remediation and a lack of aggravating circumstances.		should evaluate their systems to ensure compliance with the BSA.	
President Trump issued an Executive Order on securing the US bulk-power system. On 1 May 2020, US President Trump issued an Executive Order (EO) aimed at preventing cyberattacks to and interference by foreign adversaries on the US power grid. The EO prohibits the acquisition, importation, transfer or installation of bulk-power system electrical equipment in the US power grid if the US Department of Energy (DOE) determines that: (i) the equipment has a nexus with any foreign adversary (e.g., produced or supplied by entities subject to the jurisdiction of certain high-risk countries); and (ii) the transaction poses an unacceptable risk to national security. Under the EO, the "bulk-power system" is defined as: (i) facilities and control systems necessary for operating an interconnected electric energy transmission network or any part of the network; and (ii) electric energy from generation facilities needed to maintain transmission reliability. The EO specifically excludes facilities used in local distribution. Additionally, "bulk-power system electrical equipment" includes bulk-power system substations and control rooms, substation transformers, large generators and backup generators. Covered equipment is limited to the items specifically listed in the EO. While the EO did not provide a list of "foreign adversaries," the DOE recently issued a Request for	28 September 2020	The DOE is required to publish rules or regulations implementing the EO within 150 days of EO's issue date. This would mean that the DOE must publish rules by the end of September 2020. While proposed rules may come out this fall, the DOE will likely be unable to issue a final rule implementing the EO until 2021.	Securing the United States Bulk-Power System Executive Order DOE Notice on Securing the United States Bulk-Power System

 Immediate impact

 Short-term impact

 On the horizon

Legal issue/risk	When?	What's next	Supporting information
Information in the US Federal Register listing China, Iran, North Korea, Russia and Venezuela as foreign adversaries.			
The IRS is taking a renewed interest in compliance and fraud enforcement. On 1 October 2020, James Lee will replace Don Fort as chief of the IRS Criminal Investigation division. The IRS Commissioner described Mr. Lee as highly-respected and noted that he will build upon the working relationships with the civil side of the IRS as well as with the Department of Justice. The IRS also installed Damon Rowe, a veteran of the Criminal Investigation division, as director of the newly-created Fraud Enforcement Office. This office will technically reside within the Small Business/Self Employed Division, but will work on agency-wide compliance issues, including consulting on Fraud Enforcement strategic plans, programs and policy.	October 2020	There likely will be an increase in compliance and fraud enforcement as cooperation between the IRS civil and criminal divisions rises. Companies should prepare for increased frequency and intensity of fraud audits.	IRS Criminal Investigation veteran selected as new Fraud Enforcement Director James Lee selected to lead IRS Criminal Investigation
California residents will vote on the California Privacy Rights Act, which, if passed, will impose increased privacy obligations on businesses that process California consumers' personal information. On 3 November 2020, California residents will vote on the California Privacy Rights Act (CPRA). If approved, the CPRA will become operative on 1 January 2023, and with the exception of the right of access, shall only apply to personal information collected by a business on or after 1 January 2022. The CPRA would replace the California Consumer Privacy Act and would impose additional requirements on companies to protect California consumers' personal	3 November 2020	Companies should monitor the outcome of the 3 November 2020 election. If the CPRA is passed, companies that process California consumers' personal information should consult with counsel and take steps to implement procedures sufficient to comply with the new CPRA requirements.	California Privacy Rights Act

 Immediate impact

 Short-term impact

 On the horizon

Legal issue/risk	When?	What's next	Supporting information
information from unauthorized or illegal access, destruction, use, modification or disclosure. The CPRA also contemplates the establishment of a new data protection agency, the California Privacy Protection Agency (CPPA), which will have full administrative power, authority and jurisdiction to implement and enforce the CPRA. The CPPA is expected to issue regulations that will require businesses to perform cybersecurity risk assessments and annual audits.			
FinCEN is considering regulatory amendments intended to improve anti-money laundering programs and compliance with the Bank Secrecy Act. On September 17, 2020, the US Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") published an Advance Notice of Proposed Rulemaking ("ANPRM") seeking public comment on a variety of potential regulatory amendments to the anti-money laundering ("AML") requirements of the Bank Secrecy Act ("BSA"). The proposed rule would define an "effective and reasonably designed" AML program as one that (i) identifies, assesses and reasonably mitigates risks resulting from illicit financial activities; (ii) assures and monitors compliance with the BSA's recordkeeping and reporting requirements; and (iii) provides "information with a high degree of usefulness to government authorities consistent with both the institution's risk assessment and the risks communicated by relevant government authorities as national AML priorities." It also would explicitly require financial institutions to conduct risk assessments and would provide companies with more flexibility in allocating their resources to address evolving risks. The BSA already requires	16 November 2020	The public may submit comments on or before November 16, 2020 (within 60 days of the ANPRM's publication). FinCEN will then consider the submitted comments and may issue a final rule. In the interim, financial institutions should review their procedures for conducting risk assessments and ensure that they are effective in identifying and remediating potential issues.	Department of the Treasury Proposed Rulemaking: Anti-Money Laundering Program Effectiveness

 Immediate impact

 Short-term impact

 On the horizon

Legal issue/risk	When?	What's next	Supporting information
financial institutions to implement a compliance program that, at a minimum, includes: (1) a system of internal controls; (2) independent testing of the company's AML program; (3) designation of an AML compliance officer; (4) implementation of an adequate employee training program; and (5) risk-based customer due diligence procedures. If the proposed rule is implemented, the industries that would be affected include banks (including credit unions and other depository institutions); casinos and card clubs; money services businesses; brokers or dealers in securities; mutual funds; insurance companies; futures commission merchants and introducing brokers in commodities; dealers in precious metals, precious stones, or jewels; operators of credit card systems; loan or finance companies; and housing government sponsored enterprises.			
Virginia continues to pursue measures to enhance data privacy protections. The Virginia Data Protection and Privacy Advisory Committee is expected to discuss House Bill 954 (HB954), or the "Cybersecurity; care and disposal of customer records; security for connected devices", prior to the 2021 regular legislative session. HB954 requires any business that owns, licenses or maintains personal information about a Virginian resident, to take all reasonable steps to dispose of, or arrange for the disposal of, customer records containing personal records within its custody or control by shredding, erasing or otherwise modifying the personal information in those records to make it unreadable or undecipherable.	Ongoing	The Virginia Data Protection and Privacy Advisory Committee is expected to discuss HB954 in autumn 2020. Companies that own, license or maintain personal information about a resident of Virginia should continue to monitor developments.	Virginia HB954

 Immediate impact

 Short-term impact

 On the horizon

Legal issue/risk	When?	What's next?	Supporting information
The IRS is taking a renewed interest in high-net-worth individuals. On 15 July 2020, the IRS started to examine the tax returns of high-net-worth individuals and private foundations using data analytics to identify sophisticated tax planning and aggressive tax strategy. The Global High Wealth Industry Group, known as the IRS Wealth Squad and specially trained in complex domestic and international transactions and structures, is expected to conduct comprehensive and exhaustive audits as a part of this compliance campaign.	Ongoing	Private foundations and high-net-worth individuals should prepare for increased frequency and depth of IRS audits. With the adoption of data analytics, the IRS will be able to identify issues that have previously gone undetected.	2020 Annual Audit Plan

 Immediate impact

 Short-term impact

 On the horizon

Legal issue/risk	When?	What's next?	Supporting information
US Congress is considering a bill that would criminalize soliciting or receiving bribes and establish a process to fund overseas anti-corruption initiatives. The Russian and Other Overseas Kleptocracy (CROOK) Act was introduced in US Congress with bipartisan support. The committees assigned the bill to the full US House of Representatives and Senate for consideration on 18 December 2019, but the US Congress has not yet voted on the bill. The US Foreign Corrupt Practices Act (FCPA) criminalizes offering, paying, or promising to pay bribes to foreign officials. The CROOK Act, if passed, also would criminalize soliciting or receiving bribes. It would require 5% of fines levied in FCPA enforcement actions to be deposited into an anti-corruption "action fund," which would be used to assist overseas anti-corruption initiatives.	Ongoing	It is unclear when Congress will vote on the CROOK Act. Companies should continue to monitor developments.	H.R. 3843 – Countering Russian and Other Overseas Kleptocracy Act

Immediate impact

Short-term impact

On the horizon

Contacts

Sarah Paul
Partner

T: +12 1 23 01 65 87
sarahpaul@
eversheds-sutherland.us

Andrea Gordon
Associate

T: +12 0 23 83 09 55
andreagordon@
eversheds-sutherland.us

Pooja Kohli
Litigation Specialist

T: +12 1 23 89 50 37
pkohli@
eversheds-sutherland.us

Emily Rosenblum
Associate

T: +1 610 742 0889
emilyrosenblum@
eversheds-sutherland.us

Daniel Strickland
Associate

T: +12 0 23 83 08 97
danielstrickland@
eversheds-sutherland.us

eversheds-sutherland.com/financialinstitutions

MAN_002\9887012\2