Volume 2, Issue 1 | 2018

MOFOCUS

OUR INSIGHTS INTO THE RISK + CRISIS LANDSCAPE

IN THIS ISSUE

EDITORS

John Carlin
Partner
New York/Washington, D.C.

Robert Litt
Of Counsel
Washington, D.C.

David Newman
Of Counsel
New York/Washington D.C.

Sophia Brill
Associate
Washington, D.C.

FOLLOW US

Global Risk + Crisis Management Practice

John Carlin

SEC PUBLISHES NEW GUIDANCE AND BRINGS RELATED ENFORCEMENT ACTION

In two steps that appear to indicate renewed, if not intensified, scrutiny of public companies' cybersecurity practices by the Securities and Exchange Commission (SEC), the SEC's five commissioners unanimously issued guidance (the "Guidance") on February 21, 2018, covering a range of cybersecurity topics, including disclosure obligations, board oversight, and risk management controls. While the Commission issued the Guidance unanimously, it is important to note that two of the commissioners have released public statements expressing reserved support for the Guidance, but noting that it in large part recapitulates guidance regarding cybersecurity disclosure already presented in 2011 by the SEC's Division of Corporation Finance.

Public companies should closely review the Guidance for the additional details it provides regarding key disclosure obligations.

continued on page 2

Disclosures regarding cybersecurity threats and practices should be integrated throughout a company's periodic reports, including the Risk Factors, Management's Discussion & Analysis, Description of Business, Legal Proceedings, and Financial Statements Disclosures sections. "Companies should avoid generic cybersecurity-related disclosures and provide specific information that is useful to investors." The Guidance also advised public companies to consider disclosure regarding the nature of Board oversight of the management of risks relating to cybersecurity matters.

"Companies should avoid generic cybersecurity-related disclosures and provide specific information that is useful to investors."

While companies are not required to make specific technical disclosures that would compromise their security efforts and while the SEC recognizes that additional details may come to light in the course of ongoing security investigations, companies should make every effort to provide timely disclosures with the information at their disposal so that the public can make informed investment decisions.

The Guidance also touches upon two areas not previously discussed by the SEC:

Companies are encouraged to adopt, implement, and regularly update comprehensive cybersecurity risk management policies. Importantly, these policies should specify disclosure controls and procedures that ensure that relevant information regarding cybersecurity threats and developments are channeled to the right personnel, for purposes of both assessing risk and determining disclosures obligations. There should, in particular, be a free flow of information up the corporate ladder to senior management.

Information about cybersecurity risks and practices may be material nonpublic information, and, therefore, companies should be mindful of applicable insider trading laws when drafting codes of conduct, designing trading black-out periods, and otherwise implementing executive trading policies.

Following up on its Guidance, on April 24, 2018, the SEC settled an enforcement action against Altaba (f/k/a Yahoo!) Inc. In that settlement, Altaba agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches. Per the SEC, Yahoo's information security team became aware of the December 2014 data breach and informed Yahoo's senior management and legal department of the breach within days, but made no public disclosure for more than two years.

According to the SEC's settlement order: (1) Yahoo failed to disclose the breach or its potential business impact and legal implications in SEC filings during the two-year period following the breach; (2) Yahoo did not share information regarding the breach with its auditors or outside counsel in order to assess the company's disclosure obligations in its public filings; and (3) Yahoo failed to maintain proper disclosure controls and procedures.

In the press release announcing the settlement, the SEC staff provided insightful guidance regarding cybersecurity disclosure and SEC enforcement, with Steven Peikin, Co-Director of the SEC Enforcement Division, stating – "We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case."

In light of the Guidance and recent enforcement action, companies are advised to:

- ☑ make cybersecurity training and compliance a priority company-wide;
- ☑ review their existing periodic filing disclosures for completeness and timeliness;
- ☑ confirm that existing policies and practices call for appropriate and timely notification to appropriate senior leaders;
- ☑ ensure that auditors and outside counsel are informed of breaches in order to assess the company's disclosure obligations in its public filings;
- ☑ review their disclosure controls and procedures; and
- ☑ update their insider trading policies as necessary to expressly contemplate cybersecurity risks as potentially material nonpublic information.

continued on page 3

THE NEW IMPERATIVE TO INVESTIGATE WORKPLACE MISCONDUCT

The important ongoing national conversation about sexual harassment should serve as a wake-up call to companies, board members, and C-suite executives about the need to be proactive when confronted with allegations of harassment or other workplace misconduct. Raising serious legal and reputational concerns, many of these matters will require an investigation led by experienced employment and white-collar attorneys who can efficiently and sensitively examine the truth of claims and determine the best path forward.

Evidence suggests the risks posed by employee misconduct claims have not been top of mind for many corporations. Consider a survey released in October 2017 by the Boardlist, which maintains a directory of women board members, and data analytics firm Qualtrics. The survey, conducted in August 2017 with more than 400 board members at public and private companies participating, showed that nearly 80 percent of surveyed board members had not discussed sexual harassment at their companies. Additionally, nearly 90 percent of surveyed board members had not implemented a plan to address it and more than 80 percent of surveyed board members had not reevaluated their respective company's risks. The reason most board members gave for their inaction was a belief that sexual harassment was not a problem at their company.

It is now abundantly clear that not taking workplace misconduct issues seriously or failing to ask the right questions can be very damaging, and possibly fatal, for a company. Exhibit A, of course, is The Weinstein Company, the entertainment studio co-founded by Hollywood producer Harvey Weinstein. The allegations against Weinstein of systemic sexual abuse of dozens of women for decades appear to have brought the company to its knees, forcing it into a possible sale to avoid bankruptcy. In addition, the company is facing several lawsuits from Weinstein's accusers.

One of the lawsuits names members of the board of directors, alleging that they knew or should have known Weinstein was "unfit or incompetent" to work with the plaintiffs and "posed a particular risk of sexually assaulting them . . ." In addition, the New York State Attorney General's Office has announced that it is investigating whether any civil rights or antidiscrimination laws were broken at the company. The Weinstein Company has not publicly commented on the litigation nor the investigation.

Although an extreme example, The Weinstein Company is hardly alone in facing litigation over its management of employee misconduct. To cite just one more example: Signet Jewelers Ltd. and two of its former CEOs are facing a shareholder class action over disclosures about sexual misconduct allegations at the company's Signal division. The case stems from a report in *The Washington Post* detailing written declarations made in private arbitration proceedings by current and former Signet employees who painted a picture of a company where sexual harassment and abuse were tolerated and encouraged by its top executives. The lawsuit claims that in SEC filings and other public statements, the company "steadfastly denied and downplayed the allegations made by the plaintiffs in the arbitration" even though the arbitrator issued an interim decision in 2015 noting that "[f]or the most part Sterling has not sought to refute this evidence." The company has said that the shareholder case is without merit.

In this new environment, employee misconduct issues cannot be viewed only through the prism of employment law. Instead, they should be seen as potentially putting the entire enterprise at risk.

Beyond the financial and regulatory risks these cases demonstrate, they highlight the reputational damage companies, boards, and executives face if they do not adequately handle allegations of workplace misconduct. Reputation damage can be substantial and can negatively affect a range of important relationships involving customers, regulators, employees, and potential employees.

NEW PRISM

In this new environment, employee misconduct issues cannot be viewed only through the prism of employment law. Instead, they should be seen as potentially putting the entire enterprise at risk. In some cases, a thorough inquiry by credible outsiders with experience conducting internal investigations and dealing with government entities may be necessary.

Of course, employment law experience is essential in these matters. Understanding the company's potential legal exposure under relevant laws, such as the Title VII of the 1964 federal Civil Rights Act and the New York State Human Rights Law, and ensuring the employer protects the rights of accuser and accused

continued on page 4

during the pendency of the investigation are critical. Employment attorneys also have relevant and significant experience speaking with victims and evaluating their credibility as well as advising employers.

Nevertheless, employee misconduct issues have taken on new salience. As women—and men—are empowered to come forward with allegations of workplace misconduct, the potential for more systemic problems to be revealed will increase. These issues will involve not only the facts of the particular allegation but also who at the company knew about the alleged behavior, what they knew, and when they knew it. Combining the substantive knowledge and experience of employment attorneys with white-collar defense attorneys who routinely conduct sensitive internal investigations will ensure that these inquiries are appropriately holistic and effective.

Regulators are more attuned than ever to these issues. The New York State Attorney General Office's Civil Rights Bureau, for example, has the authority to investigate—and often brings civil actions—against companies for patterns and practices of harassment or discrimination that often affect large groups of people. The bureau recently updated its guidance about laws that protect New Yorkers from sexual harassment in the workplace.

"No New Yorker should be forced to walk into a workplace ruled by sexual harassment, intimidation, or fear," New York Attorney General Eric Schneiderman said in a statement this past December.

The New York State Attorney General Office's investigations have led to significant monetary settlements. In 2015, for example, it, along with U.S. Equal Employment Opportunity Commission, announced a $3.8 million settlement with the Consolidated Edison Company of New York, Inc., to resolve allegations of sexual harassment and discrimination against women field workers by co-workers and supervisors. Notably, the New York State Attorney General's Office found that the company failed to address the widespread harassment and discrimination.

KEY ELEMENTS TO INTERNAL INVESTIGATIONS

When allegations of employee misconduct surface within a company, the most prudent response in many cases will be to conduct an internal investigation to determine the facts, including whether the underlying conduct is part of a broader pattern at the company. Further, under Title II and similar state civil rights laws, investigations are not only wise but required as part of the employer's obligation to prevent and promptly correct discrimination or harassment. Done correctly, an investigation can assure key constituencies—employees, regulators, customers, board members, business partners—that the company takes the allegations seriously and that the allegations have been addressed fairly and fully.

Internal investigations, however, can cause unforeseen damage if not done correctly. It is beyond the scope of this article to outline every element needed for a successful internal investigation, but two fundamentals are worth highlighting.

After months of news about employee misconduct across many industries, it appears that our culture has reached an inflection point. It is imperative that the business community demonstrates that it understands the gravity of this moment.

Credible and experienced investigators. Historically, many companies have chosen to handle their own internal investigations of employee misconduct issues. The degree of in-house expertise and the quality of their investigations vary from excellent to nonexistent. In this new climate, however, in-house investigations, regardless of the quality of the investigators, could be particularly vulnerable to criticism, especially when high-profile employees are involved. An internal investigation attacked (legitimately or not) as a whitewash could make matters worse for the company by potentially damaging its credibility with key stakeholders, such as an alleged victim of misconduct, triers of fact, prosecutors, and rank-and-file employees. By engaging outside counsel with sufficient independence and credibility, companies can blunt this kind of criticism.

A clearly defined work product. It is also critical to know what type of final work product will result from the internal investigation and for whom it is intended. Initially, it is prudent to decide whether a privileged report will be produced that can be withheld from both the accuser and the accused, with the option of waiving privilege as needed. Throughout an investigation, lawyers make many complex decisions about what kind of information they are willing to share with other third parties, including opposing parties in litigation and regulators or prosecutors, implicating other questions about work product and attorney-client privilege. Accordingly, lawyers must carefully consider whether there should be a final report and, if so, whether it should be written or oral.

CONCLUSION

After months of news about employee misconduct across many industries, it appears that our culture has reached an inflection point. It is imperative that the

continued on page 5

business community demonstrates that it understands the gravity of this moment. To inspire confidence with their key constituencies and appropriately handle what could become a particularly sensitive and damaging matter, companies should seriously consider turning to attorneys with the needed credibility and experience investigating sensitive and complex matters to bring about a satisfactory resolution.

RECENT CYBERCRIME BUST PAINTS 'STRIKING PICTURE' OF 'DARK-WEB' OPERATION

Adapted from CNBC article – https://www.cnbc.com/2018/02/22/russian-cybercrime-bust-and-how-fight-the-hackers-commentary.html

On February 7, the Department of Justice unsealed a sweeping indictment against 36 defendants for their role in the "Infraud Organization." The indictment reads at times like a 21st century crime novel, giving the public an insight into the size, sophistication, and discipline of criminal cyber networks operating online (something well known to those who track these organizations).

The indictment also shows how U.S. law enforcement agencies are striking back in concert with partners around the world in an effort to raise the cost of doing business for these types of outfits.

According to the allegations in the indictment, Infraud was launched in 2010 by defendant Svyatoslav Bondarenko of Ukraine and served as a central clearinghouse that allowed members to traffic in stolen identities, financial and banking information, malware, and other online contraband. Over the course of seven years, the indictment alleges, the site grew to more than 10,000 members across the world and caused more than half a billion dollars in losses to consumers, businesses, and financial institutions.

Meeting threats such as this takes a serious investment in technological safeguards as well as a willingness to adapt to an evolving threat. Beyond the operation's scale, the striking picture that emerges from the indictment is the degree to which Infraud operated very much like a dark-web cousin of major commercial marketplace sites.

The group's leadership imposed a rigid hierarchy to maintain order on the site, delegating authority to system administrators and other associates who held roles of varying responsibility ranging from "Moderators" to "Super Moderators" to "Administrators." It also relied on a system of strictly enforced rules and user-generated feedback to maintain quality control. Longstanding site members were promoted to "VIP Member" status to honor their contributions and solicited advice on the "In Fraud We Trust" discussion forum.

Given Infraud's worldwide membership, U.S. law enforcement needed to partner with others across the world to effectuate the arrest and to send a meaningful warning to wrongdoers in the future: The unsealing of the indictment followed the arrests of 13 individuals in the United States and six other countries (Australia, the United Kingdom, France, Italy, Kosovo, and Serbia).

In its public statement, the Justice Department offered thanks to a long list of cooperating law enforcement agencies around the world without whom "[t]he international operation to dismantle the Infraud Organization would have been impossible."

Conspicuously absent from the list is Russia, even as the indictment gives indications that the site itself was being hosted in Russia. Among other things, the indictment alleges that in 2011 the site's founder issued a decree that banned the buying and selling of contraband involving Russian victims, a tactic experts noted is used to discourage Russian law enforcement from taking down a Russian-hosted server.

While these types of multi-jurisdiction arrest sweeps are intended to send a message to cyber-criminals, the most important message in the near term is for the public: In today's environment, companies are up against not just solo hackers, but highly skilled enterprises that rely on an international collection of criminal and cyber expertise.

A new report from the White House Council of Economic Advisers estimated that malicious cyber activity cost the U.S. economy as much as $109 billion in 2016 and emphasized that even though "government can help address some elements of cyber protection issues, the most direct actions in cybersecurity are in the hands of the private sector."

Meeting this threat takes a serious investment in technological safeguards as well as a willingness to adapt to an evolving threat. Companies and individuals should invest now in protections against these kinds of threats and begin planning for scenarios in which their systems are breached and their information finds its way to these kinds of dark corners of the internet.

continued on page 6

OFAC'S NEW RUSSIA-RELATED SANCTIONS

On April 6, 2018, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) added 38 new designees to its list of Specially Designated Nationals and Blocked Persons ("SDN List") related to Russia pursuant to Presidential Executive Orders (EOs) 13661 and 13662. Specifically, in an effort to counter Russian "elites who profit from a corrupt system" and a government that engages "in a range of malign activity," OFAC's sanctions targeted 7 wealthy Russian individuals, 12 companies deemed to be owned or controlled by those individuals, 17 senior Russian government officials, and a Russian weapons trading company and its subsidiary Russian bank.

A critical aspect of the new sanctions is that foreign persons may be affected by the new designations by virtue of the Countering America's Adversaries Through Sanctions Act (CAATSA), which was signed by President Trump on August 2, 2017 and provides for mandatory sanctions against any person, including non-U.S. entities and individuals, that knowingly engages in "significant transactions" with SDNs designated under applicable laws.

Among industries most heavily affected by the new sanctions are metals traders (particularly aluminum traders), energy, banking, and finance. Given the extensive operations that many of the new SDNs have within western economies, it is anticipated that these sanctions will have a significant effect on the sanctioned entities and on companies that engage in significant transactions with these SDNs.

Provided below is a discussion of how the new Russia sanctions may affect both U.S. and non-U.S. persons.

REQUIREMENTS OF U.S. PERSONS AND FOREIGN PERSONS UNDER THE NEW DESIGNATIONS

U.S. persons (defined to cover U.S. companies, U.S. citizens, permanent resident aliens, and any persons within the United States) are prohibited from engaging in or facilitating transactions with SDNs, including entities that are 50% or more owned by one or more SDNs. Non-U.S. persons can also be subject to sanctions for facilitating a "significant transaction" with respect to SDNs related to U.S. sanctions on Russia by virtue of CAATSA.

The full list of new designees can be found here: https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180406.aspx.

OFAC GENERAL LICENSES AND WIND-DOWN PERIOD

General License 12

In connection with the new SDN designations, OFAC issued General License 12, which authorizes activities "ordinarily incident and necessary to the maintenance or wind down of operations, contracts, or other agreements … that were in effect prior to April 6, 2018" through 12:01 a.m. EST on June 5, 2018. It is important to note that the scope of General License 12's wind-down activities is limited to the specific entities identified on General License 12. Thus, General License 12 does not cover transactions related to Rosoboronexport, the Russian weapons trading company designee, and Russian Financial Corporation, its subsidiary Russian bank designee.

Additionally, U.S. persons seeking to rely on General License 12 are subject to the following conditions:

- Any payments due to an SDN that are permissible under General License 12 must be deposited into a blocked bank account in the United States. U.S. persons can receive payments from the SDNs covered by the General License relating to arrangements with the SDNs covered under General License 12 entered into prior to April 6, 2018.
- U.S. persons must report to OFAC on actions taken under General License 12 within 10 business days of its expiration on June 5, 2018.

According to OFAC's FAQs, U.S. person employees are permitted to provide services to, and receive salary payments, pension payments, or other benefits from, the blocked entities untilJune 5, 2018, "if such activities are ordinarily incident to the continuity of operations or to facilitate a wind-down." Similarly, General License 12 may allow U.S. companies who had placed an order for goods with a designee (or its 50%-owned company) prior to April 6, 2018 to accept such goods until June 5, 2018.

General License 13

OFAC also issued General License 13, which authorizes U.S. persons to conduct activities "ordinarily incident and necessary" to divesting or transferring debt, equity, or other holdings of three of the designees (specifically, EN+ Group plc, GAZ Group, and United Company RUSAL plc) through May 7, 2018. Authorized activities include facilitating, clearing, and settling transactions to divest debt, equity, or other holdings in such blocked entities to non-U.S. persons. However, General License 13 does not permit U.S. persons holding accounts or other property for a new SDN to unblock such accounts or property. As with General License 12, U.S. persons

continued on page 7

undertaking transactions authorized by General License 13 must report such transactions to OFAC within 10 business days of its expiration on May 7, 2018.

OFAC'S 50% RULE

Under OFAC's "50% Rule," an entity that is 50% or more owned by one or more SDNs is also deemed an SDN, even if the entity is not specifically listed on OFAC's SDN List. As a result, companies transacting with entities that may be commercially connected to the newly sanctioned SDNs should conduct diligence beyond screening against OFAC's SDN List to ensure that the counterparty to a transaction does not have a corporate ownership structure suggesting that an SDN is its beneficial owner.

The 50% Rule also applies to the entities listed on General Licenses 12 and 13. Thus, transactions that are authorized under the General Licenses are also authorized for entities 50% or more owned by the entities identified in the applicable General License.

APPLICABILITY OF NEW SANCTIONS TO U.S. PERSONS

U.S. persons are prohibited from engaging in or facilitating any transaction in which an SDN has an interest. Thus, except as expressly authorized by General License 12 or 13, or pursuant to an OFAC specific license, OFAC can impose sanctions on U.S. persons for engaging in any transaction with an SDN, regardless of dollar value.

EXTRATERRITORIAL APPLICATION OF NEW SANCTIONS

As a general matter, non-U.S. persons are not prohibited from engaging in transactions with SDNs. However, under CAATSA, U.S. sanctions related to the new Russian SDN designations apply extraterritorially.

Section 228 of CAATSA amended the Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 (SSIDESA) by adding a new Section 10 that requires the President to impose sanctions on:

> *"a foreign person if the President determines that the foreign person knowingly, on or after the date of the enactment of [CAATSA] —*
>
> *(1) materially violates, attempts to violate, conspires to violate, or causes a violation of any license, order, regulation, or prohibition contained in or issued pursuant to any covered Executive order, [SSIDESA], or the Ukraine Freedom Support Act of 2014 (22 U.S.C. 8921 et seq.); or*
>
> *(2) facilitates a significant transaction or transactions, including deceptive or structured transactions, for or on behalf of—(A) any person subject to sanctions imposed by the United States with respect to the Russian Federation; or (B) any child, spouse, parent, or sibling of an individual described in subparagraph (A)."*

As part of the FAQs released on April 6, OFAC noted that in determining whether a transaction by a foreign entity is a "significant transaction," the agency will examine the transaction under a subjective "totality of the facts and circumstances" test. We note that notwithstanding the listed factors considered under this test (such as the size of the transaction, the nature of the transaction, and management's awareness of a "pattern of conduct"), OFAC has considerable discretion in determining when a transaction becomes significant enough to subject a foreign person to sanctions.

The Russian SDN designations also implicate other provisions of CAATSA with extraterritorial applicability. For example, Section 5 of the Ukraine Freedom Support Act of 2014 (UFSA) gave the President discretion to impose sanctions on Russian and other foreign financial institutions that "facilitated a significant financial transaction on behalf of any Russian person included on" the SDN List pursuant to UFSA or any applicable Executive Order, unless waived by the President as being "in the national security interest of the United States." However, Section 226 of CAATSA amended this section to make such sanctions mandatory (though the President maintains the ability to waive such sanctions). OFAC guidance on the implementation of Section 5 of UFSA notes that OFAC will generally interpret the term "facilitated" broadly.

PRACTICAL CONSIDERATIONS

Companies that are engaged in transactions in which a Russian SDN may have an interest will need to be cautious and undertake appropriate diligence to confirm that the transaction does not violate the new OFAC sanctions. For example, a U.S. company cannot use a broker to indirectly acquire products from a Russian SDN, as it would be prohibited from doing so directly. Similarly, a non-U.S. company that engages in transactions with the Russian SDNs can be subject to sanctions if OFAC determines that such transactions are significant.

Thus, persons and entities potentially covered by the scope of the applicable sanctions' regimes should have appropriate procedures in place to comply with existing sanctions and monitor developments to ensure ongoing compliance.

continued on page 8

CLOUD ACT WILL OVERHAUL U.S. LAWS FOR OBTAINING DATA STORED OVERSEAS

The CLOUD Act, which was signed into law on March 23, will significantly change the rules governing certain types of data stored overseas by U.S. businesses. Passed as part of a 2,232-page spending bill, the CLOUD Act addresses a question that U.S. tech companies and other digital service providers have long been grappling with: May the U.S. government compel a company operating in the United States to produce data that it stores outside the country?

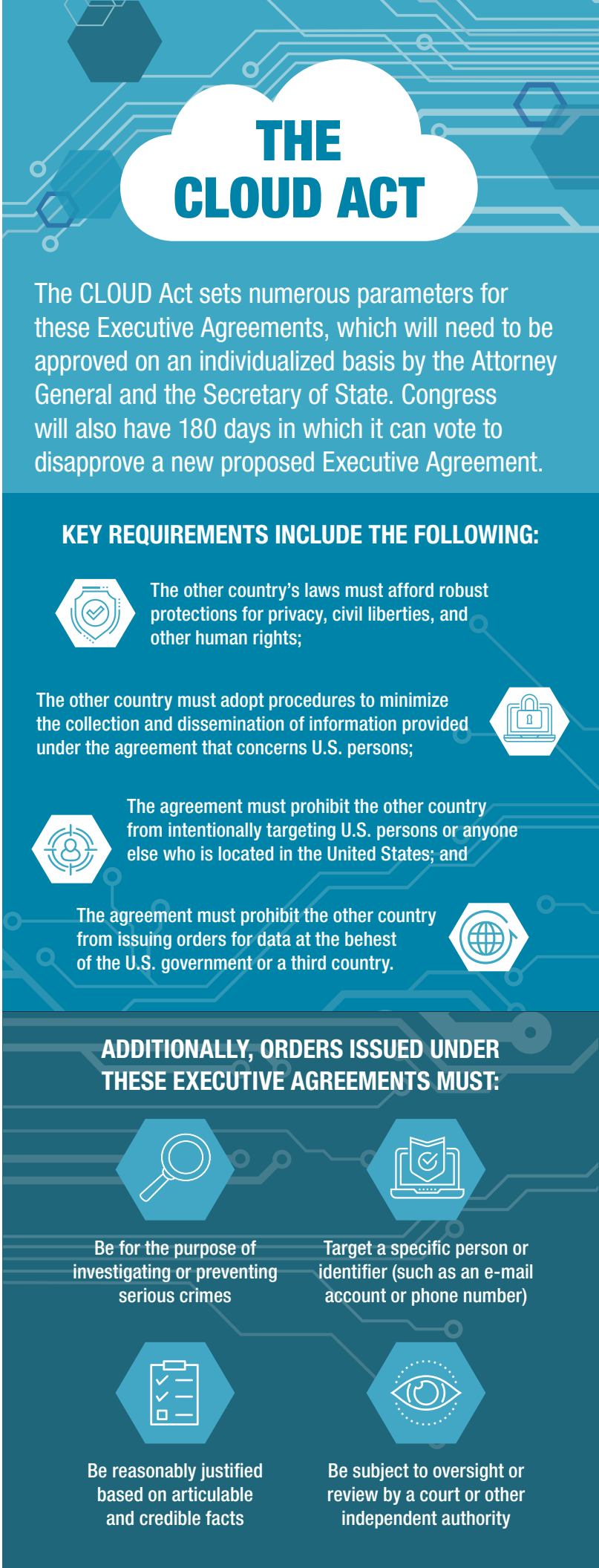
The CLOUD Act makes clear that in the case of legal process served under the Stored Communications Act (SCA), which applies to certain types of digital service providers, *see* 18 U.S.C. §§ 2701 *et seq*., the answer is yes. The law will also allow U.S. businesses covered by the SCA to respond to certain foreign governments' requests for records that are stored here in the United States.

U.S. clients should be aware that businesses covered by the SCA may now be ordered to disclose records regardless of where the records are stored, provided that all of the other requirements of the law are met. If the U.S. government enters into certain Executive Agreements with other countries, clients covered by the SCA may also be permitted to disclose records held in the United States pursuant to orders issued by foreign governments.

U.S. LAW ENFORCEMENT REQUESTS FOR DATA HELD OVERSEAS

The first part of the CLOUD Act (short for "Clarifying Lawful Overseas Use of Data") requires U.S. companies that are served with court orders under the SCA to turn over data no matter where the data is stored—so long as it is within the U.S. company's "possession, custody, or control." The CLOUD Act now effectively moots the question that was presented in the *United States v. Microsoft*: It leaves no doubt that the SCA applies to data stored overseas by companies subject to jurisdiction in the United States.

However, clients should be aware that the SCA does not apply to all types of businesses or all types of data. It applies to providers of "electronic communication services" and "remote computing services." Generally speaking, these terms include businesses that facilitate electronic communications by customers (e.g., e-mail or electronic messaging) and businesses that provide members of the public with computer storage services (e.g., cloud computing services). *See* 18 U.S.C. §§ 2510(15), 2711(2). The types of records sought can



include the contents of stored communications as well as information about individual subscribers.

The CLOUD Act also contains a provision that U.S. tech companies strongly supported: It allows providers served with orders or subpoenas under the SCA to file a petition to modify or quash the order or subpoena if the provider reasonably believes that (1) the target of the request is not a U.S. person and does not reside in the United States; and (2) the required disclosure creates a material risk that the provider would violate the laws of another country with which the U.S. government has an Executive Agreement (discussed in the next part below). A court can quash the subpoena or order if it finds that both of these factors are met and that the overall interests of justice favor the provider's challenge. The statute lists a number of considerations that must be taken into account in the interests-of-justice assessment, including considerations of international comity.

Providers may also be able to raise international comity-based challenges where an order would force the provider to violate the laws of another country with which the United States does *not* have an Executive Agreement. In that circumstance, the provider's arguments would have to be based on common law comity considerations rather than any provision of the CLOUD Act. The government has taken the position that such challenges can be pursued only in the context of a contempt proceeding, rather than by motion to quash the subpoena or order.

REQUESTS BY FOREIGN GOVERNMENTS FOR DATA HELD IN THE UNITED STATES

The CLOUD Act's second component will allow the U.S. government to enter into Executive Agreements with other countries that will permit U.S. companies covered by the SCA and other provisions of the Electronic Communications Privacy Act to respond to those other countries' requests for data. This aspect of the legislation resembles a proposal introduced by the Obama administration in 2016, which was designed to enable data-sharing between the United States and the U.K.

Under the SCA as it currently stands, a U.S. company subject to the SCA that is served with a court order or other request for data by a foreign government is generally prohibited from complying. The CLOUD Act changes this by permitting these types of businesses to respond to requests from foreign governments that have entered into an Executive Agreement with the United States.* For example, if an Executive Agreement between the United States and the U.K. is reached, a U.S. company that is subject to the U.K.'s jurisdiction could be served with an order under the laws of the U.K. to produce customer data; if that data is stored in the United States (and provided the U.K. order complies with the requirements of the CLOUD Act), the company would be permitted to disclose it.

In sum, the CLOUD Act significantly alters the legal landscape for U.S. businesses covered by the SCA when they are served with requests by the U.S. government for data that they store overseas. It will also significantly change the rules for U.S. businesses covered by the SCA that are served with requests by other governments for data that is stored here. The impact of this second part of the law, however, will only become effective once the U.S. government begins entering into Executive Agreements with other countries.

* Service providers would also be permitted to conduct live interceptions of communications—i.e., wiretaps—pursuant to orders from foreign governments, subject to a set of additional requirements described in the legislation.

BUG-BOUNTY PROGRAMS: A VALUABLE TOOL TO BE USED CAREFULLY

A wide range of organizations have embraced vulnerability-disclosure programs (VDPs) that actively encourage members of the public to hack into their own company systems. Under a VDP, a company invites "good" or "ethical" hackers to explore the company's systems and then to report back about any discovered weaknesses. The information reported is then used to fix the vulnerability and to implement stronger protections going forward. A form of VDP surging in popularity is the bug-bounty program (BBP) in which financial or other incentives are offered to outsiders for reporting relevant information.

BBPs have come into favor because they represent a cost-effective "force multiplier" that can augment existing efforts a company may be pursuing to identify and remediate vulnerabilities. Companies are understandably attracted to the idea of making a $500 payout (the approximate average reward for a discovered bug of any severity) as an alternative to enduring an incident that could ultimately cost millions of dollars. Some companies see such programs as a lower-cost complement to increasing investment in internal security measures. Even large institutions that make substantial investments in internal security experts recognize the value of enlisting outside actors with a new perspective to stress test and supplement those efforts.

As the benefits of having a BBP have become widely known, a growing range of companies have decided to adopt them. Such programs are no longer the

continued on page 10

exclusive province of technology companies, including giants like Google, but also include retail and service companies, such as Starbucks. Over the past year, we have seen companies of all sizes and industries institute these types of programs to good effect.

Notably, the U.S. government has joined these efforts with programs such as "Hack the Pentagon," a bug-bounty program instituted by the U.S. Department of Defense in 2016 after a successful pilot. As then-Secretary of Defense Ash Carter observed, "We know that state-sponsored actors and black-hat hackers want to challenge and exploit our networks. . . . What we didn't fully appreciate before this pilot was how many white-hat hackers there are who want to make a difference, who want to help keep our people and our nation safer."

While there are considerable benefits to gain from having a BBP, companies must be careful in how they design and implement these programs to avoid legal and reputational risk. Both the design phase of the program as well as the response to specific reports can pose challenges that must be navigated carefully. Based on what we have observed, there are several topics organizations must pay special attention to:

- **When designing the program, think carefully about what network components and data to include and consider making sensitive information off limits.** This point was emphasized in Department of Justice (DOJ)-issued guidance on VDPs. Entities must consider a number of factors when deciding what should be included within the scope of a BBP. Such factors include the sensitivity of the information, the safeguards already in place, and any applicable regulatory or contractual restrictions. To the extent an organization decides to include within its BBP a system that contains sensitive information, organizations might consider implementing technical methods that prevent participants from being able to access the information.
- **When drafting the publicly available policy for the program, be clear on the scope of authorized conduct.** It may be useful, for instance, to prohibit participants from engaging in any intentional conduct that changes user-generated data, impairs or disables systems, or that otherwise makes data inaccessible or includes the downloading of any company information. Not only does this clarity avoid creating questions later in a civil-suit context about what may have been "authorized" through its program, it also removes a potential impediment to DOJ bringing a criminal case under the Computer Fraud and Abuse Act arising out of a malicious hack of the company's systems.
- **Consider what federal agencies have stated about VDPs.** DOJ is not the only federal agency thinking seriously about VDPs. The Federal Trade Commission, National Highway Traffic Safety Administration, and Food and Drug Administration have issued guidance on best security practices that include consideration of VDPs.
- **Decide in advance what proof is needed to confirm a hack.** Companies also should specify how that information should be shared with them.
- **Assign a central point of contact to receive vulnerability disclosure reports and be clear about which personnel are authorized to answer questions about the program.** It is easier to respond to unusual reports and difficult questions if there is a clear point of reference for report processing. Questions that raise new and unanticipated legal issues should be handled carefully.
- **Be clear and transparent about whether and how you will pay a bounty.** This means setting reward amounts for different discoveries. Additionally, while some organizations offer cash rewards, others, like Massachusetts Institute of Technology, offer alternative perks.
- **Only pay a bounty if it is for an activity that is specifically authorized by your policy.** It is important to create rules and to follow them closely. Otherwise, a company might put itself into an unfavorable negotiating position with participants.
- **Consider using test accounts.** This will help to ensure that customer data is not unnecessarily compromised through the BBP.
- **Consider a third-party host.** Depending on the company, there may be value to using a third-party platform to host the program.

Each organization is different in terms of the types of information it holds, the legal regimes to which its information is subject, and the contractual and other obligations that may restrict disclosure. Additional legal issues arise where a company stores data or conducts activities outside the United States. The International Organization for Standardization and the International Electrotechnical Commission published standards on designing VDPs and, like DOJ, recommend that any company that adopts a VDP obtain legal advice in order to ensure that their programs are consistent with local laws.

continued on page 11

The bottom line is that BBPs are a valuable tool that should be carefully designed and deployed to maximize benefits and reduce risks to the organization. The above lessons should not dissuade organizations from giving BBPs serious consideration. But they highlight the value in taking time to design and implement the programs thoughtfully.

THE KREMLIN'S ONLINE ACTIVITIES GO FAR BEYOND ELECTION MEDDLING. THE U.S. NEEDS TO FIGHT BACK.

Adapted from Politico article - https://www.politico.com/magazine/story/2018/02/27/russia-election-meddling-rogue-state-217094

In four different instances in recent weeks, the U.S. government, often with allies throughout the world, has publicly called out Russia's bad online behavior and made clear it is behaving as an outlaw nation.

The loudest condemnation, of course, came in the form of Special Counsel Robert Mueller's recent indictment of the Russian Internet Research Agency and 13 individuals involved in interfering from afar with the 2016 presidential election—a highly detailed, 37-page document that reads like an espionage novel, complete with covert trips, stolen identities, and faked on-the-ground recruiting in states from New York to Florida.

Mueller's indictment, echoing the assessment of every high-level Trump administration national security official, leaves no doubt that Russia engaged in a large, lengthy, and expensive effort to interfere with our democratic process, an effort that involved scores of employees who showed up at their office job each day to undermine our tradition of democratic elections. And it's not just Mueller who is warning us about the Kremlin's increasingly nefarious activities.

Vladimir Putin's Russia is engaged in a low-intensity conflict not just against the United States but against the civilized world, where commerce and prosperity are inextricably intertwined with digitally connected machines. Fearing that both democracy and free and fair economies represent an existential threat to his corrupt authoritarian regime, Putin's Russia is increasingly responsible both for indiscriminate destructive cyberattacks and for harboring cybercriminals who harm the global online economy. It is impossible to confront threats to cybersecurity without addressing the Putin problem.

Less discussed, just days before Mueller's indictment, the so-called Five Eyes—the intelligence alliance between the U.S., U.K., Canada, New Zealand, and Australia—named Russia responsible for last year's devastating NotPetya ransomware attack, which was responsible for hundreds of millions of dollars in damages to companies around the world.

"We saw an indiscriminate attack launched by Russia against Ukraine in the ongoing hostilities there. What they used was a cyberweapon that was launched in the dark, that hit numbers of companies, individuals, and caused damage to our economies. It stopped shipping from moving . . . it literally shut [companies] down," White House cybersecurity coordinator Rob Joyce said. "And that is unacceptable."

The NotPetya attack caused massive disruptions at companies as varied as the shipping company FedEx ($300 million in damages), drugmaker Merck ($310 million in damages), and the advertising firm WPP ($15 million in damages). It required the replacement of 45,000 computers and 4,000 servers at the cargo giant Maersk alone. "We can't blame the victims for something a nation state wantonly did in an act of aggression," Joyce said. "Russia needs to be held responsible for this."

Earlier, on February 7, the Justice Department unsealed charges against 36 individuals who ran and participated in a massive online crime forum called Infraud—run from within the protection of Russian borders for the better part of a decade—that facilitated more than $530 million in losses by stealing and trading credit card numbers. The forum's motto was clear about their goal: "In Fraud We Trust." (See more on the Infraud charges above.) Thanks to well-meaning and like-minded international law enforcement partners, more than a dozen of those targeted were arrested, in countries that included Australia, the United Kingdom, France, Italy, Kosovo and Serbia. It's no surprise that those indicted in Russia remain at large.

Just days before the Infraud indictment, Russian hacker Peter Levashov—one of the most notorious spammers in the internet's history—was extradited to a Connecticut courtroom from Spain, where he was captured while on vacation after years of living safely in Russia. Russia vigorously protested his arrest and tried hard to return him to its soil rather than see him face justice in the United States.

The collective message is hard to miss: Putin's Russia is a rogue actor, and both its government's behavior

continued on page 12

and the freedom it provides criminals is making the world less safe. It is operating far outside the bounds of civilized countries online. It's a problem similar to the rogue behavior we're seeing from North Korea on nuclear issues—and we need a similar, collective global approach to punish and isolate Russia.

"Russia is ripping up the rulebook by undermining democracy, wrecking livelihoods by targeting critical infrastructure and weaponizing information," British Defense Secretary Gavin Williamson said, in citing Russia's role in NotPetya. "We must be primed and ready to tackle these stark and intensifying threats."

If Russia harbored terrorists whose attack caused FedEx $300 million in damages, or if the Russian government attacked a FedEx transit hub, our retaliation would be swift and decisive. It must be the same in cyberspace. Russia's behavior is undermining the consumer trust and posing a systemic risk to an increasingly wired world, particularly as we move more of our infrastructure and daily life online, from cars to medical devices.

InFraud is only the latest in a long series of such online crime forums, including CarderPlanet.Ru, led by the Russian hacker Roman Seleznev, who was eventually captured overseas when he left Russia and was sentenced last year to decades in U.S. federal prison.

There are many more like Seleznev to catch. Today's list of Most Wanted CyberCriminals is a who's who of Russian hackers. Among others, there's Evgeniy Bogachev, the creator of the GameOver Zeus botnet and architect of a vast financial fraud that stole somewhere north of $100 million from U.S. banks and businesses, and Alexsey Belan, who has been indicted in three major cybercrimes, most recently along with another criminal and two Russian FSB intelligence officers who were involved in the theft of a billion user accounts from Yahoo. Putin enables these online bazaars and shields their leaders from criminal prosecution—or, worse, as appears to be the case with both Belan and Bogachev, signs up criminals as intelligence assets, to help enable further thefts and espionage by the government.

It's critical the White House and U.S. government punish Russia. President Barack Obama created a mechanism to sanction states that participated in malicious cyber behavior and then used it, in December 2016, against Russia after its election operations. But more needs to be done—and the United States needs to take the lead. The most effective action is collective action. The United States needs to partner with countries around the world to impose devastating economic penalties proportional to the billions of dollars of indiscriminate criminal cyber-enabled activities and for the repeated undermining of internal democratic elections around the world. The partnership of the interconnected world should also consider collectively closing embassies and consulates.

The threat from efforts like the Internet Research Agency is hardly behind us; these attacks on our country and our democracy are ongoing. The very same week that the NotPetya condemnations and Mueller's indictment became public, proving the depths of Putin's Russia's depravity, Twitter trolls and bots linked to Russia were busy promoting conspiracy theories and online discord related to the murder of children in Parkland, Florida.

Then in late February came news that U.S. intelligence has concluded that Russia attacked the opening ceremonies of the Olympics—the very epitome of an event and moment aimed at a peaceful, collaborative global community. What could demonstrate more tellingly that Putin's regime is fundamentally opposed to the rest of the civilized world than attacking the opening ceremonies of the Olympics, a celebration by 92 countries from every corner of the globe? According to private-sector reports, it appears the Olympics attack was carried out by the same GRU unit responsible for helping to spread NotPetya.

Responsible countries cannot allow this behavior online to continue without response. Failure to act encourages worse and worse behavior—and not just by Putin's Russia: Other rogue regimes are watching and wondering where the lines are for cyber aggression. One of the lessons of America's battle against terrorism is that we cannot allow terrorists safe havens inside ungoverned or poorly governed countries around the world; we must develop a similar doctrine to ensure the world's safety online. Against Russia, those tools could range from further sanctions to frozen international bank accounts to cyber activity intended to target the infrastructure used by criminals and efforts like the Internet Research Agency.
