Table of Contents

<table>
<thead>
<tr>
<th>Tab</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>California SB1-Plus? GDPR-Like?</td>
</tr>
<tr>
<td>B</td>
<td>States Respond to Equifax Cyber Breach with Enforcement Actions and Calls for Enhanced Regulatory Powers</td>
</tr>
<tr>
<td>C</td>
<td>FFIEC Statement Regarding OFAC’s Cyber-Related Sanctions Program Risk Management</td>
</tr>
</tbody>
</table>
California SB1-Plus? GDPR-Like?
Considerations for Financial Institutions in Evaluating the California Consumer Privacy Act

Nathan D. Taylor and Purvi G. Patel

05/24/2018

Privacy + Data Security, Financial Services, Financial Institutions + Financial Services, Banking + Financial Services, Financial Services Litigation, Financial Services Enforcement, and Financial Technology

Client Alert

This alert was also published in Law360 on May 30, 2018.

Financial institutions in the United States are no strangers to privacy regulations, particularly given the obligations imposed by the federal Gramm-Leach-Bliley Act ("GLBA") and the California Financial Information Privacy Act ("SB1"). More recently, financial institutions have been focused on whether and/or the extent to which the EU's GDPR may apply to their U.S. operations. Many financial institutions, however, have yet to consider an equally important U.S. privacy development—the California Consumer Privacy Act ("Act"), a ballot initiative likely to appear on the November ballot. [1]

If approved by voters, the Act would impose notice obligations on covered businesses to disclose the categories of personal information ("PI") they collect, sell, and share about California consumers, and give those consumers a right to say "no" to the "sale" of their information. [2] We discussed the Act and its potential requirements and related risks, including litigation arising from alleged violations of the Act, in greater detail in an earlier alert.

Here, we highlight certain considerations that are unique to financial institutions and evaluate the potential impact of the Act on financial institutions, particularly given their existing privacy obligations under the GLBA and SB1. Below are six key considerations for financial institutions to keep in mind as they navigate the interplay between the Act, the GLBA, and SB1. 

1. No GLBA or SB1 Exception.

Although the Act includes a Fair Credit Reporting Act ("FCRA") exception for consumer report information, the Act does not include an exception for financial institutions or for compliance with the GLBA or SB1. [3] That is, the Act fails to recognize that financial institutions doing business in California are already subject to both a comprehensive federal financial privacy regime (the GLBA) and the most significant state financial privacy regime (SB1). Nor does the Act otherwise acknowledge the existing notice obligations and disclosure limitations to which financial institutions are already subject. As a result, financial institutions doing business in California that meet one or more of the Act's applicability criteria (e.g., annual gross revenue beyond $50 million) would be subject to the Act's requirements. [4]

2. Difference in Scope Between the Act and the GLBA and SB1.

While there are many distinctions between the GLBA, SB1, and the Act, the most basic (but nonetheless critical) distinction is the types of individuals they respectively protect. The GLBA and SB1 both apply to information about individuals who obtain financial products and services for personal, family, or household purposes. [5]
The Act, however, would apply more broadly to information about individuals who are California residents. [6] It is similar to California’s data security and breach notification laws in this regard, [7] applying to information about Californians generally, regardless of their relationship to a business. As a result, a covered financial institution would be subject to the Act’s various privacy obligations with respect to not only its customers who are California residents, but also any other California resident regarding whom the financial institution collects PI, including, for example, an employee or vendor who is a California resident.

3. The Relevance to Existing GLBA Notice Requirements.

There are two types of “notice” requirements under the Act. First, a covered business would be required to include various Act-related disclosures in, among other things, “any California-specific description of consumers’ privacy rights.” [8] For instance, a business would be required to update—at least annually—the list of the categories of PI it has collected, sold to a third party, or disclosed for business purposes. [9] If a financial institution includes a disclosure in its GLBA privacy notice that is specifically for California residents (e.g., a “For California residents” statement in the “Other Important Information” section of its GLBA notice), [10] the financial institution would have to consider whether that disclosure would be considered a “California-specific description of consumers’ privacy rights” and, if so, whether the financial institution is required to address the Act’s disclosure requirements in its GLBA privacy notice (in addition to any notice that it may prepare specifically to address the Act).

The Act, however, goes beyond traditional concepts of macro-level, privacy-related disclosures that focus on listing generally applicable examples or categories of information or activities. For example, upon a consumer’s request, a covered business would be required to identify by category the PI that the business has sold to a third party and has disclosed for business purposes in the preceding 12 months, as well as “provide accurate names and contact information” for the recipients of that information. [11]

The consumer “right to know,” particularly as it pertains to PI disclosed for a business purpose, is far reaching, and implicates the everyday transactions that a financial institution undertakes for its customers. A transaction, by definition, involves multiple parties, and banks must disclose customer PI in order to provide the very financial products and services requested by a customer. To illustrate, when a bank’s customer uses her credit card online to pay for a purchase, the bank will receive the authorization request through the relevant payment card network. Regardless of whether the bank authorizes or declines the request, the bank must communicate its authorization decision to the relevant payment card network so that information can then be communicated back to the merchant. As a result, the Act’s “right to know” provisions could require a financial institution to engage in a burdensome administrative and recordkeeping process to track every recipient (and its contact information) to whom it has disclosed data relating to a California resident pertaining to routine business purposes.


The GLBA and SB1 provide a consumer with some control over the extent to which a financial institution can disclose information about the consumer to a nonaffiliated third party. Specifically, the GLBA gives consumers the right to opt out of a financial institution’s disclosure to nonaffiliated third parties, while SB1 only permits a financial institution to share information with nonaffiliated third parties if a customer opts in to such sharing. [12]

But, a consumer’s rights under the GLBA and SB1 are not “absolute.” More specifically, both the GLBA and SB1 include sensible exceptions to their respective opt-out and opt-in requirements to facilitate the types of non-controversial
disclosures that a financial institution must make to run its business and provide the very financial products and services requested by consumers. [13] In particular, both the GLBA and SB1 include exceptions that permit a financial institution to disclose information for activities like fraud prevention, maintaining and servicing accounts, and processing transactions. [14] To the extent a GLBA or SB1 exception applies, a financial institution may disclose information about a consumer, regardless of whether the customer has exercised a GLBA opt-out or has not opted in under SB1.

In contrast, the Act’s broad scope and limited exceptions would functionally create a far more “absolute” consumer right to opt out of the “sale” of information than exists under either the GLBA or SB1, separately or together. The Act does not include any practical exceptions with respect to its opt-out right for the “sale” of information similar to those found in the GLBA and SB1. This is critical because of the Act’s extremely broad definition of the term “sale,” which includes “sharing . . . a consumer’s [PI] with a third party, whether for valuable consideration or for no consideration, for the third party’s commercial purposes.” [15]

This aspect of the definition of “sale” is focused on disclosures that are for the recipient’s “commercial purposes,” presumably as distinct from the business purposes of the entity disclosing the information. A financial institution would have to evaluate the extent to which it shares information with third parties for the third party’s commercial purposes, notwithstanding the fact that the financial institution may receive no compensation (and may not even consider the disclosure to be a “sale,” as that term is commonly understood). For example, if a consumer applies for a mortgage with Bank A, and Bank A contacts Bank B (with which the consumer has a checking account) to confirm that the consumer has sufficient funds to cover her down payment in the mortgage transaction, would Bank B’s disclosure to Bank A be considered a disclosure for Bank A’s “commercial purposes,” a disclosure for Bank B’s “business purposes,” or both?

The combination of the Act’s expansive definition of “sale” and lack of the types of exceptions found in the GLBA and SB1 would create an important inconsistency among the three privacy regimes. The challenge here will be reconciling disclosures that are otherwise permitted under the GLBA and SB1 and those that a consumer will be able to opt out of under the Act.

5. Affiliate Sharing Implications and Potential Preemption Challenges.

On its face, the Act does not appear to differentiate between sharing consumer PI with an affiliate—whether through a sale or a disclosure for a business purpose—and sharing with a non-affiliate. [16] If the Act’s broad definitions of “sale” and “third party” [17] limit the ability of a financial institution to disclose information to an affiliate, the Act may conflict with the FCRA and be vulnerable to preemption challenges.

There is precedent in this regard. After the passage of SB1, the American Bankers Association, The Financial Services Roundtable, and Consumer Bankers Association sued the California Attorney General and others asserting that the FCRA’s affiliate-sharing preemption provision preempted the affiliate-sharing provision of SB1. [18] The trade associations prevailed on that claim to the extent that SB1 sought to limit the sharing of information permitted under the FCRA. A similar challenge could be raised against the Act to the extent it attempts to limit the sharing of information with an affiliate that the FCRA permits.

6. Indirect Implications for Fraud Prevention and Other Purposes.

The Act’s right to “say no” to the sale of consumer PI could present operational challenges for a financial institution, [19] regardless of whether the financial institution is subject to the Act. Financial institutions often rely on non-FCRA, third-party
data products to evaluate applications, process transactions, and otherwise engage in “core” financial service activities. A financial institution may purchase non-FCRA data in various contexts, such as:

- A bank may obtain a fraud report in evaluating an application for credit;
- A bank may obtain information relating to whether a computer device attempting to log in to online banking has previously been associated with fraud; or
- A bank may obtain an Office of Foreign Assets Control (“OFAC”) report in the context of evaluating an application to open a deposit account or a wire transfer request on an existing account to ensure that the underlying transaction would not be prohibited by anti-money laundering and anti-terrorist financing provisions under federal law.

If the financial institution seeks the above information for a California resident who has opted out of the sale of her information by the data provider from which the financial institution requests the information, the financial institution would not be able to obtain the information (assuming, of course, that the information is not a consumer report subject to the FCRA).

Even more troubling, because the Act does not have a fraud prevention exception to its opt-out right, fraudsters and other criminals residing in California would be able to functionally “clean” non-FCRA fraud databases by exercising their opt-out rights, thereby impairing the value of critical information on which financial institutions rely to prevent fraud and money laundering and to comply with the law.

Financial institutions should pay close attention to the Act and this year’s ballot initiative process. If the initiative is successful, financial institutions will need to consider the extent to which existing GLBA and SB1 procedures will need to be modified to address the Act. Moreover, financial institutions will need to put in place new privacy processes to provide California consumers with accurate disclosures regarding the sale and disclosure of PI.

[1] On May 3, 2018, proponents of the California Consumer Privacy Act announced they had collected the number of signatures needed to qualify the Act for the November ballot. https://ballotpedia.org/California_Consumer_Personal_Information_Disclosure_and_Sale_Initiative_(2018). Before the Act can be included on the ballot, however, county election officials must verify the signatures, and the Secretary of State must certify the measure qualifies for the ballot.

[2] See §§ 1798.100–1798.102. Unless otherwise specified, all citations are to Section 4 of the initiative measure, and track proposed changes to the California Civil Code.


[5] See 12 C.F.R. § 1016.3(e)(1) (defining a “consumer,” in pertinent part, as “an individual who obtains or has obtained a financial product or service . . . that is to be used primarily for personal, family, or household purposes”); Cal. Fin. Code § 4052(f) (SB1) (defining a “consumer,” in pertinent part, as “an individual resident of this state . . . who obtains or has obtained from a financial institution a financial product or service to be used primarily for personal, family, or household purposes”).
§ 1798.106(g) (defining “consumer” as a “natural person who is a California resident”).

See Cal. Civ. Code §§ 1798.81.5(a)(1) (noting the intent of the California legislature to require that “personal information about California residents is protected”), 1798.82(a) (requiring notice to “a resident of California” for certain security incidents involving personal information relating to the individual).

§ 1798.104(a)(5).

Id.


§ 1798.104(a)(4).

See 12 C.F.R. § 1016.10 (GLBA); Cal. Fin. Code § 4052.5 (SB1).


§ 1798.106(q).

§§ 1798.101(a), 1798.104(a)(4), 1798.106(l), (s).

§ 1798.106(q), (s).

Am. Bankers Ass’n v. Lockyer, 541 F.3d 1214 (9th Cir. 2008).

§ 1798.102.
States Respond to Equifax Cyber Breach with Enforcement Actions and Calls for Enhanced Regulatory Powers

October 13, 2017

In the wake of last month’s historic cyber breach of Equifax, which resulted in the theft of sensitive personal information belonging to over 140 million Americans,¹ states have wasted no time in seeking a greater role in regulating cybersecurity risk. Historically, while state consumer agencies and attorneys general have enforced notification requirements for victims of cyberattacks where consumer data was compromised, significant enforcement actions have been the purview of federal agencies such as the Federal Trade Commission, the U.S. Department of Justice, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. However, given the scope of recent breaches and the sensitivity of the information that was stolen, states have recently stepped up and launched their own investigations and enforcement actions, and have imposed new data protection standards on various types of businesses. Assuming this trend continues, organizations responsible for defending against cyberattacks, or who find themselves the victim of a successful hack, may find themselves with both federal and state cyber regulators to deal with.

I. Massachusetts Brings the First Enforcement Action

Since the announcement of its data breach, on September 7, 2017, Equifax has faced a barrage of criticism from regulators, litigants, and Congress on its failure to adequately secure its information systems against attack, as well as its multi-week delay in disclosing the breach to consumers and the investing public. On September 19, 2017, the Commonwealth of Massachusetts took this criticism a step further and filed a civil action against Equifax for failing to adequately protect consumer data and for other related violations.²


In the complaint filed by Massachusetts Attorney General Maura Healey, Equifax is alleged to have (i) failed to adopt appropriate safeguards of customer data, as required by Massachusetts regulations regarding data security; (ii) failed to provide timely notice of the data breach to the state and to affected consumers, as required by the state’s data breach notification law; and (iii) engaged in unfair and deceptive trade practices based on, among other things, the company’s failure to abide by its own promises to consumers regarding its data security policies and procedures, in violation of the state’s consumer protection law.3

The Massachusetts action focuses on Equifax’s alleged failure to implement the widely-available security patch to the Adobe Struts application, which is believed to have contributed to the vulnerability. Specifically, the complaint alleges that, in early March 2017, the developers of the Adobe Struts application as well as cybersecurity watchdog groups notified the public of a severe vulnerability in the application that would leave systems using it vulnerable to hacking. Notwithstanding this notice, Equifax allegedly failed to implement an available security patch to the application, which was released in early March 2017. Equifax’s system was reportedly first breached two months later, in May 2017, by hackers who took advantage of the Adobe Struts vulnerability. Equifax did not detect the breach until late July 2017. The lawsuit further alleges that Equifax faltered in its response to the breach by failing to ensure that adequate call center staffing and online resources were available to answer questions from affected consumers, and by improperly seeking to make a profit from consumers by charging for certain credit protection services beyond a one-year period.

According to AG Healey, customers have experienced and will continue to experience significant financial losses, lost time, and aggravation as a result of Equifax’s alleged misconduct. The State of Massachusetts is seeking injunctive relief, civil penalties, restitution and legal costs.

II. Multiple States Launch Investigations and Demand Information

In addition to the Massachusetts lawsuit, attorneys general in New York, Illinois, California, and in other states announced investigations of Equifax, with AG Schneiderman of New York declaring the purpose was getting to “the bottom of how and why this massive hack occurred.”4


States have a variety of tools at their disposal to investigate and penalize companies for data breaches. For example, most states in addition to the District of Columbia and certain U.S. territories have data breach notification laws that generally require prompt notification to consumers and/or state regulators of data breaches that affect the personal information of those states’ residents. These notification laws typically allow state attorneys general to bring enforcement actions for non-compliance.

In New York, for example, the attorney general may seek to recover any consequential damages suffered by consumers who were entitled to notice but were not notified, as well as a fine of up to $150,000 if the failure to provide notice was knowing or reckless. A smaller number of states have laws that expressly require companies to adopt certain cybersecurity measures to protect the personal data of their residents. In New Mexico, for example, companies that fail to adopt “reasonable security procedures and practices” may be sued by the attorney general for actual damages caused by a company’s failure to maintain such safeguards as well as receive a fine of up to $150,000 for knowing or reckless violations. Finally, some states rely on pre-existing consumer protection laws, which usually prohibit deceptive or unfair trade practices, to pursue companies for damages, penalties, and injunctive relief for either (i) failing to adopt appropriate safeguards for consumer data or (ii) misleading customers about the existence or strength of the company’s cybersecurity safeguards.

Further, on September 19, 2017, the attorneys general and consumer protection regulators from over forty states signed a letter to Equifax that expressed “profound concerns” regarding the breach, primarily concerning the rollout of Equifax’s consumer notice of the data breach and offer of free credit monitoring to consumers. These concerns include (i) language that initially appeared in the terms of service that required customers to agree to an arbitration clause and class action waiver as a condition of accepting the free credit monitoring; (ii) Equifax’s marketing of fee-based identity protection services alongside its offer of free identity protection services, which could potentially deceive consumers into selecting the fee-based service; and (iii) Equifax’s failure to provide sufficient call center support and internet resources, such that consumers reported being unable to obtain additional information regarding the breach.

---

5 See N.Y. GBS § 899-aa.6(a), https://www.nysenate.gov/legislation/laws/GBS/899-AA.
8 Equifax ultimately removed the arbitration language and declared that it would not seek to compel any consumers into arbitration. See https://www.equifaxsecurity2017.com/2017/09/13/progress-update-consumers-4/.
These same state attorneys general have also turned their attention to Experian and TransUnion, the other two major credit reporting agencies. Although there is no evidence that these other credit reporting agencies were affected by the Equifax breach, on October 10, 2017, the state attorneys general demanded that the other credit agencies voluntarily waive the fees they charge consumers—often $10—to impose or lift credit freezes, noting (i) that consumers must seek credit freezes from all three credit reporting agencies in order to fully protect themselves from the Equifax breach and (ii) that it is inappropriate for these credit agencies to impose fees for credit freezes, given that consumers do not voluntarily choose to do business with credit reporting agencies.

III. New York Calls for Expanded Regulatory Powers

New York’s Attorney General and Governor have also used the Equifax breach as an opportunity to impose new and tougher cybersecurity standards on credit agencies such as Equifax as well as any business that handles the private information of New York residents.

A. Renewed Call for Passage of New York Data Security Act

On September 15, 2017, AG Schneiderman wrote in an op-ed article that he was renewing his call for the passage of the New York Data Security Act, which would require New York businesses to implement and maintain data security programs. AG Schneiderman had previously proposed the legislation in January 2015, but it failed to gain traction. If enacted, the law would implement the following cyber-related provisions.

- **Data Security Standards and Programs.** Any entity that does business in New York and maintains certain private information regarding New York residents would be required to develop, implement and maintain “reasonable safeguards” to protect the confidentiality of that information. Entities would also be required to implement an information security program that includes: (i) administrative safeguards, such as conducting risk assessments and training employees; (ii) technical safeguards, such as assessing risks in network and software design; and (iii) physical safeguards, such as protecting against unauthorized access to private information during collection, transportation, destruction, and disposal.

---


• **Broad Definition of Private Information.** The definition of private information would be expanded beyond standard forms of personal information, such as social security numbers, to also cover biometric information, unsecured protected health information, and a username or email address in combination with a password or security question and answer that would permit access to an online account.

• **Safe Harbor and Law Enforcement Sharing.** To encourage compliance with the new standards, a rebuttable presumption of compliance would be provided if an entity’s cybersecurity program is certified annually by an independent third party auditor. The legislation would also offer immunity from liability in a civil action, including an action brought by the attorney general, for entities that comply with certain information security guidelines published by the National Institute of Standards and Technology. In addition, the bill would incentivize companies to share information about data breaches with law enforcement by establishing that the production of forensic reports to local and state law enforcement agencies for the purpose of investigating a breach is not a waiver of any privilege or protection, such as the work product doctrine or trade secret protection.

• **Penalties and Enforcement.** The New York Attorney General would be empowered enjoin violations and seek civil penalties of $250 for each person whose private information was compromised, up to a maximum of $10 million per breach. For violations found to be knowing or reckless, these amounts increase to $1,000 for each affected person, up to the greater of $50 million or three times the aggregate amount of any actual costs and losses.

**B. Proposed Oversight of Credit Reporting Agencies**

On September 18, 2017, Governor Cuomo directed the New York Department of Financial Services (“DFS”) to implement new regulations that would expand the jurisdiction of the DFS, which regulates financial services firms and insurance companies, to include credit reporting agencies, such as Equifax, that collect data on consumers in New York.13 The proposal would mandate that credit reporting agencies not only register with the DFS but also comply with the DFS’s “first-in-the-nation” cybersecurity rules.14

Under the proposal, credit reporting agencies that collect information on consumers in New York would be required to register with the DFS and would be subject to DFS’s cybersecurity rules. The credit reporting agencies would also be subject to ongoing DFS examinations and investigations to evaluate compliance. Should a credit reporting agency or its officers fall out of compliance, or

---


otherwise appear to be “not trustworthy and competent to act as or in connection with a consumer credit reporting agency,” the DFS could suspend or revoke the credit reporting agency’s registration and thereby prohibit the firm from doing business with consumers and certain financial institutions in New York.

Under the proposal, consumer credit reporting agencies would be required to register with the DFS by February 1, 2018, and would have a phased period to comply fully with the cybersecurity regulations by October 4, 2019.

IV. Conclusion

Even before the Equifax breach, states had begun taking an increasingly active role in penalizing companies that failed to safeguard consumer information.15 However, the scope of the Equifax breach is likely the tipping point that will call states to more muscular action, including more aggressive statutes, compliance examinations, and enforcement actions. As a result, businesses must be increasingly mindful of not just federal data protection standards and rules, but of increasingly strict state rules as well. Businesses that possess sensitive data that cybercriminals might seek to exploit would do well to regularly revisit their cybersecurity controls, policies, and procedures to ensure that they comply with all applicable laws.

Please feel free to contact any of the following Cadwalader attorneys if you have any questions about this memorandum.

Joseph Moreno  +1 202 862-2262  joseph.moreno@cwt.com
Joseph Facciponti +1 212 504-6313  joseph.facciponti@cwt.com
Peter Carey  +1 202 862-2339  peter.carey@cwt.com

---

Joint Statement

Office of Foreign Assets Control Cyber-Related Sanctions Program Risk Management

The Federal Financial Institutions Examination Council (FFIEC) members\(^1\) developed this statement to alert financial institutions to recent actions taken by the Department of Treasury’s (Treasury) Office of Foreign Assets Control (OFAC) under OFAC’s Cyber-Related Sanctions Program and to the potential impact that sanctions may have on financial institutions’ operations, including the use of services of a sanctioned entity.

This statement is intended for information only and does not contain any new regulatory expectations. This statement highlights that compliance with OFAC sanctions can impact information technology and other operations. Additional information on requirements and expectations regarding OFAC-related compliance is available from OFAC. Institutions may refer to the FFIEC Information Technology (IT) Examination Handbook for additional information regarding operational risk management.

BACKGROUND

OFAC implemented the Cyber-Related Sanctions Program on April 1, 2015, in response to Executive Order 13694 and a related declaration of a national emergency to address the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States caused by the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by, entities located, in whole or in substantial part, outside the United States.\(^2\) Since the program’s inception, OFAC has issued sanctions against entities who are responsible for, are complicit in, or that have engaged in, certain malicious cyber-enabled activities, including by providing material and technological support to malicious cyber actors that have targeted U.S. organizations. Some of the sanctioned entities claim that they are U.S.-

\(^1\) The FFIEC comprises the principals of the following: the Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

\(^2\) [https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf](https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf)
based and offer services to financial institutions. U.S. persons are generally prohibited from engaging in transactions with sanctioned entities and all property and interests in property of the sanctioned entities subject to U.S. jurisdiction are blocked (i.e., frozen).

**RISKS**

Continued use of products or services from a sanctioned entity, directly or indirectly through a service provider, may increase operational and OFAC compliance risk for a financial institution and could result in violations of law, civil money penalties, enforcement actions, and damage to the financial institution’s reputation.

**RISK MITIGATION**

Financial institutions should ensure that their OFAC compliance and risk management processes address the challenges arising from possible interactions with a sanctioned entity. Identifying, assessing, and mitigating any risks associated with these sanctions requires a high degree of collaboration across a financial institution’s OFAC compliance, fraud, security, IT, third-party risk management, and risk functions to assess any potential risk.

**OFAC Compliance Program Risk Assessment**

The Executive Order may increase OFAC sanctions compliance risk for some U.S. financial institutions. Financial institutions should assess their individual OFAC sanctions compliance risks and identify potentially impacted relationships and transactions. Additionally, financial institutions should ensure that their sanctions screening systems are updated and confirm that they have processes and procedures in place to comply with these sanctions.

Continued use of products and services from a sanctioned entity may cause the financial institution to violate OFAC sanctions. These sanctions prohibit U.S. persons — including U.S. financial institutions — from conducting transactions with sanctioned entities. Prohibited transactions include trade or financial transactions and other dealings, which may be broadly interpreted to include technical transactions such as downloading a software patch from a sanctioned entity.

Given the complexities of some of these third-party relationships and transactions relative to the sanctions, affected financial institutions are encouraged to contact OFAC, their legal counsel, and/or their security offices for additional guidance.

---

---

4 | Prohibited transactions are trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute. See [OFAC’s FAQ](https://www.treasury.gov/resource-center/sanctions/OFAC-Faq/Pages/faq.aspx).

5 | Blocking immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regard to the property. See [OFAC’s FAQ](https://www.treasury.gov/resource-center/sanctions/OFAC-Faq/Pages/faq.aspx).
Operational Risk Management

In addition to the violation of an OFAC sanction, continued use of software and technical services from a sanctioned entity may increase cybersecurity risk for a financial institution. Security software often operates within sensitive areas of an organization’s infrastructure to identify vulnerabilities, ensure data is protected, or block malware. Because of the nature of the claims under OFAC’s Cyber-Related Sanctions Program, a financial institution should assess the risk of having or continuing to use software and services from a sanctioned entity, and take appropriate corrective action.

Third-party service providers also may have used, or continue to use, products and services of a sanctioned entity on behalf of a financial institution. Accordingly, a financial institution should understand how its third-party service providers ensure compliance with the OFAC requirements.6

In some cases the sanctioned entity may be providing a critical service or control that cannot be discontinued instantly. If the products or services of a sanctioned entity provide a vital or necessary control, a financial institution should identify and implement an alternative solution at the earliest possible time. Financial institutions should contact OFAC for additional guidance as soon as possible if they encounter any operational issues related to sanctions deadlines. Financial institutions can reach OFAC through its telephone hotline at 1-800-540-6322 or by email at ofac_feedback@treasury.gov.

ADDITIONAL RESOURCES

The following government resources provide assistance to institutions for managing cyber-related sanctions risk.

OFAC Cyber-Related Sanctions Program
https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf

OFAC FAQs: General Questions

OFAC - Sanctions Programs and Information
https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

Sanctions Related to Significant Malicious Cyber-Enabled Activities
https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx

6 https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_037.htm
FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet
https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

FFIEC Information Technology Examination Handbook, Information Security Booklet
https://ithandbook.ffiec.gov/it-booklets/information-security.aspx