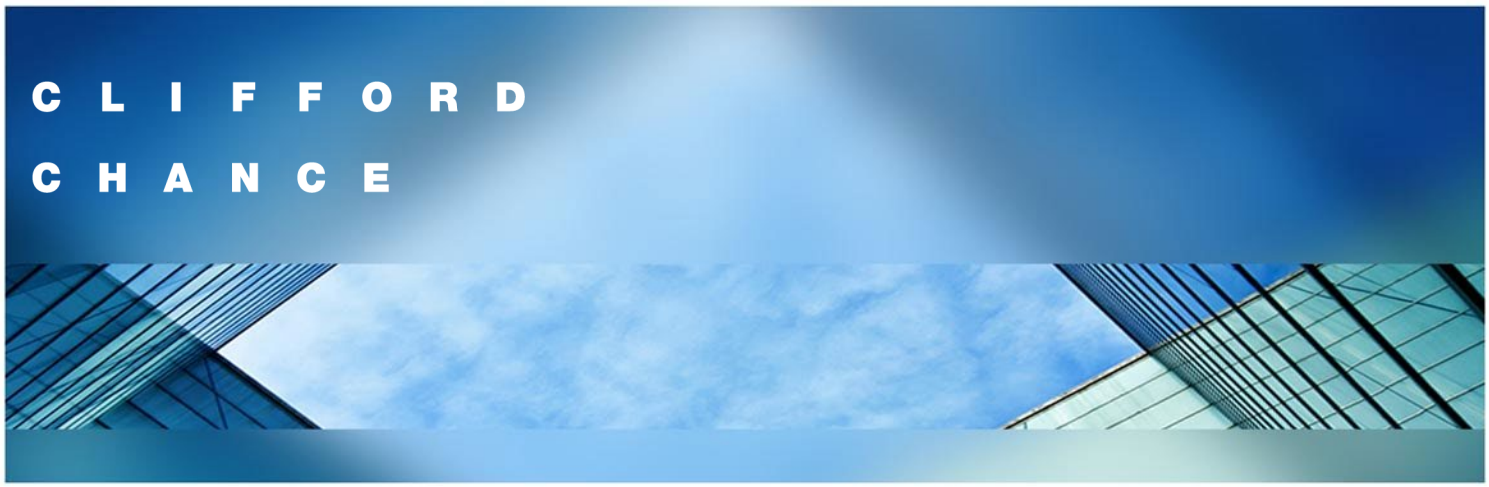

U.S. FEDERAL BANKING AGENCIES ISSUE RULE REQUIRING BANKS TO NOTIFY REGULATORS OF CYBER INCIDENTS WITHIN 36 HOURS

On November 18, 2021, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (FDIC), (the "Agencies"), issued a final rule requiring banking organizations to notify their primary federal regulator of significant computer-security incidents no later than 36 hours after determining the incident has occurred. The rule also requires bank service providers to notify their banking organization customers of any computer-security incident that has caused, or will likely cause, significant disruption. The rule imposes substantial new cyber security reporting requirements on banks with an effective compliance date of May 1, 2022.

Current rules only require reporting of certain categories of cyber incidents (such as breaches of sensitive customer information) and generally permit longer reporting periods. For example, banks must report incidents involving sensitive customer information to their primary federal regulator as soon as possible, but there is no specific deadline. Indeed, the Agencies noted in guidance accompanying the rule that notifications made under existing standards were often delayed – and in many cases banks did not report cyber incidents at all. Thus, the Agencies determined that heightened notification standards were warranted to allow for better coordination and supervision of incident response.

BANKING ORGANIZATIONS' OBLIGATION TO REPORT

Under the final rule, banking organizations must report to their primary federal regulator any "computer-security incident" that rises to the level of a "notification" incident as soon as possible and no later than 36 hours after the incident occurs. "Banking organizations" include federal and state licensed banks, federal and state savings associations, US branches of foreign banks, and bank and thrift holding companies.

What Types of Incidents Do I Have to Report?

The rule only requires banking organizations to notify their regulator of a computer-security incident that rises to the level of a "notification" incident. A notification incident is an incident that has, or is reasonably likely to, "materially disrupt or degrade" a banking organization's: (1) ability to provide services to "a material portion of its customer base;" (2) business lines, the failure of which "would result in a material loss of revenue, profit or franchise value;" or (3) operations, the failure of which "would pose a threat to the financial stability of the United States."

The Agencies provided several examples of what they consider to be "notification" incidents:

- a large-scale distributed denial of service attack that disrupts customer accounts for an extended period (four hours in the provided example);
- a failed system upgrade that results in widespread user outages for customers and employees;
- a computer hacking incident that disables banking operations for an extended period; or a ransom malware attack that encrypts a core banking system of backup data.

Notably, these examples make clear that the reporting requirement does not just apply to external attacks—internal incidents may also require reporting if they result in material disruptions or degradations to customer service.

When Do I Need to Report?

The rule requires reports to be made within 36 hours, but this timeframe does not begin until a banking organization determines a notification incident has occurred. Guidance from the Agencies makes clear that they do not consider the clock to necessarily start when the incident occurs. Rather, the Agencies anticipate that banking organizations will need to take a reasonable amount of time to investigate and determine that an incident rises to the level of a notification incident before the 36-hour clock starts.

Several commenters objected to the 36-hour timeframe, advocating for a 72-hour requirement to align with the reporting requirements of the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation and the EU General Data Protection Regulation (GDPR). However, the Agencies ultimately determined the shorter 36-hour timeframe to be appropriate in light of the high threshold for reporting and the relatively limited information that is required to be included in a report.

What Goes in a Report?

The rule requires banking organizations to provide their regulator with only a "simple notice" when they suffer a reportable incident. This notice is limited to "general information" about the incident that is known at the time the notification is made. There are no specific requirements with regards to what information is contained in the notification. In the report accompanying the rule, the Agencies explained that they intentionally kept the notification requirements minimal to

facilitate prompt reporting and to lessen the administrative burden on affected organizations.

Are My Reports Public?

The notification, and any information related to the incident, would be subject to the applicable agency's confidentiality rules, which provide protections for confidential, proprietary, supervisory, and sensitive personally identifiable information. However, the Agencies are still required to respond to individual FOIA requests, which could implicate the reported information, on a case-by-case basis.

BANK SERVICE PROVIDERS' OBLIGATION TO REPORT

The final rule also affects bank service providers, who often provide technological infrastructure services that may be subject to cyber incidents. Under this regulation, a bank service provider will be required to notify each affected banking organization as soon as possible when it determines a computer-security incident has occurred that has, or is reasonably likely to, "materially disrupt or degrade" covered services provided for four or more hours. A "covered service" is any service that is subject to the Bank Service Company Act, which includes check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, online and mobile banking, data processing, and other clerical, bookkeeping, accounting, statistical, or similar functions.

The Agencies expect bank service providers to work together with their banking organizations to designate a method of communication and point of contact that works best for both parties. In the absence of a point of contact, notification should be made to the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means.

The Agencies intend for this notification requirement to be "simple and flexible" and expect bank service providers to make their best effort to notify the banking organizations as soon as possible, so the banking organization can determine if the incident qualifies as a notification incident, triggering its own reporting requirement.

TAKEAWAYS

This rule represents a significant new regulatory obligation for banking organizations and bank service providers. While the reports themselves need not be detailed, ensuring that accurate information is provided quickly in the aftermath of a cyber incident can be difficult. Importantly, however, the Agencies narrowed the definition of a reportable incident in the final rule to only include incidents that cause actual, rather than potential harm, and excluded violations of internal policies that do not otherwise have a disruptive impact.

The Agencies estimate there will be approximately 150 notification incidents reported annually but acknowledge this number may increase in the future. The Agencies arrived at this estimate after reviewing Suspicious Activity Report (SAR) filings from 2019 and 2020, which they acknowledge do not capture the full scope of incidents addressed by the final rule, and by analyzing the frequency at which

notification incidents have already been voluntarily reported by banking organizations.

The final rule becomes effective April 1, 2022 but has a compliance date of May 1, 2022, to allow organizations additional time to implement the rule. Before the rule becomes effective, affected financial institutions should update their incident response plans to ensure that information regarding significant cyber incidents is promptly escalated to internal stakeholders who can determine if notification is required. Banks should also work with their service providers to develop notification protocols, including a designated point of contact, preferred method of communication, and specify the key information to be included in a report. Relevant service agreements should be updated to incorporate these notification requirements.

Clifford Chance has published a number of reports to help financial institutions and other companies protect themselves from cyber attacks and comply with international reporting requirements. For more information, see our Report on What Cyber Regulators Are Saying Around the World as well as our Ransomware Playbook.

CLIFFORD CHANCE

CONTACTS

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Philip Angeloff
Counsel

T +1 202 912 5111
E philip.angeloff
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Shannon O'Brien
Law Clerk (Not Yet Admitted)

T +1 212 880 5709
E shannon.obrien
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.