PUBLICATION

The Year Ahead: Privacy and Cybersecurity Issues Facing Financial Institutions in 2021

Authors: Alexander Frank Koskey, III, Matthew George White
January 11, 2021

The financial services industry faced unprecedented cybersecurity and privacy challenges in 2020. From learning how to operate with a remote workforce, dealing with a complex and evolving regulatory environment, facing an exponential rise in the number and sophistication of cyberattacks – particularly ransomware attacks and the significant and still unfolding breach of the federal government – and navigating COVID-19 issues, the cyber resilience of financial institutions was tested to its limits.

These challenges continue to exist as we enter the new year, yet 2021 brings a new set of challenges that are likely to substantially impact financial services companies in the year ahead. The incoming Biden administration is expected to place increased focus on data privacy issues, which would represent a stark contrast from the prior administration. Indeed, it's anticipated that debate around the development of a federal privacy law may intensify. At the state level, many privacy laws that stalled during the pandemic are expected to regain momentum. California continues to lead the pack after passing the California Privacy Rights Act (CPRA), which further expands consumer rights, creates additional compliance hurdles for financial institutions, and establishes the nation's first privacy enforcement agency. This could also be the year that we finally see changes to the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and potentially new requirements for financial institution incident reporting, both of which would have a significant impact on information security programs.

Beyond legislation, financial institutions will face a litany of other privacy and cybersecurity issues, including the persistently increasing threat of cyber attacks, the rise in consumer rights and awareness to data privacy at both domestic and international levels, and the need for an increased focus on vendor management. This alert will highlight some of the key privacy and cybersecurity issues that financial institutions are likely to face in 2021 and provide some practical advice on how you can be best prepared to respond.

If you would like additional information concerning any of the issues addressed in this alert, please register for our upcoming webinar on the 2021 Privacy Landscape: An overview of the issues, threats, and regulations financial institutions need to know about this year. This will be the first webinar in our 2021 monthly series examining key cybersecurity and privacy issues facing financial services companies.

New Year New Administration: What Should We Expect?

The incoming Biden administration is fully expected to bring increased attention to data privacy issues. Across the board, changes in federal agency leadership will likely result in increased consumer protections and rights, which would be a significant shift from the Trump administration. Existing federal agencies are also likely to be reorganized and fully staffed, which could lead to more regulations, examinations and enforcement actions. The Biden administration is also likely to be more active in developing federal privacy legislation, and given the new Democratic control of Congress, there might be a change after years of stalemates. There could also be increased coordination internationally with Europe and other foreign regimes on privacy issues as those countries continue to develop their privacy regimes.

By all accounts, there will be significant staffing continuity between Biden's administration and the administration of President Obama, which had previously created the federal privacy counsel. This continuity may result in increasing the efficiency and speed with which Biden's staff can move forward with privacy-related goals. Vice-President Elect Kamala Harris was also leading efforts in privacy-related issues when she served as California Attorney General, so the incoming administration possesses significant data privacy experience at the top. This represents a stark contrast with the Trump administration, which did not prioritize privacy-related policies in its legislative agenda. The increased focus on privacy could also result in more activity from regulating entities such as the FTC, FCC and CFPB.

While the pandemic will initially take top priority for the Biden administration, the challenges wrought by COVID-19 have highlighted a number of areas ripe for additional privacy protections, including remote learning, telework, contact tracing and visitor screening/data collection. These issues may encourage legislators to move forward with federal privacy legislation. Over the past few years, both sides of the aisle have examined potential federal legislation and have drafted prospective legislation. However, efforts have largely stalled due to disagreements over state preemption rules and private rights of action for privacy violations. The recent results in Georgia's Senate runoff, resulting in Democratic control of Congress, will certainly influence those negotiations and may provide a way for this legislation to move forward.

Finally, the "Schrems II" decision from the Court of Justice of the European Union invalidated the U.S. Privacy Shield, which was a primary method used by U.S. businesses to transfer data from Europe. The result severely limited the methods that can be used to effectuate data transfers, and new protocols must be established. The Biden administration may be better able to work with European leaders to help navigate a workable protocol for such transfers. Beyond Europe, China's draft privacy law presents another major need for the administration's diplomatic attention. Several other countries are also continuing to push forward efforts to develop privacy legislation.

For these reasons, expect to see data security and privacy occupy a prominent place in the list of priorities for the incoming Biden administration.

California Stays in the Spotlight

Although new privacy legislation may be on the horizon in several states, the focus as 2021 begins remains on California. Less than one year after the California Consumer Privacy Act (CCPA) went into effect, Californians voted to pass the California Privacy Rights Act (CPRA) last November. The CPRA effectively amends the CCPA and expands the consumer privacy rights of California residents, which were already the broadest in the country. In addition, the CPRA creates the California Privacy Protection Agency, the first privacy-specific regulator in the U.S.

While the CPRA does not go into effect until January 1, 2023, it contains a "look back" period beginning January 1, 2022. Therefore, any personal information collected from that point forward will be subject to the CPRA. The CPRA implements a number of substantial changes that are likely to create additional compliance hurdles for financial institutions. These include a new category for "sensitive personal information" and a consumer's right to limit the disclosure of such information, new restrictions on the ability to share data with third parties, and additional protections for the data of minors.

The CPRA's broad substantive changes mean that financial institutions must perform a comprehensive review of their policies and procedures, data collection practices, vendor agreements and more in order to comply with the CPRA's requirements. With the "look back" period less than a year away, financial institutions must make sure that CPRA compliance is at the forefront of their privacy objectives for this year. In addition, financial institutions cannot forget about their ongoing obligations under the CCPA, which currently remains in effect. Covered financial institutions, in addition to complying with the notice and consumer rights provisions of the

CCPA, must also comply with its annual requirements, including updating privacy policies and lists of personal information collected, shared and sold in the preceding 12 months.

Financial institutions doing business in California need to ensure they are complying with applicable CCPA requirements in 2021 and must now also assess whether the CPRA alters their obligations in California. For more information on the CPRA, see our prior analysis.

Potential Facelift for GLBA: Proposed Amendments

This may be the year that we finally see amendments to the Gramm-Leach-Bliley Act (GLBA). In 2019, the Federal Trade Commission (FTC) proposed amendments to the GLBA's Safeguards Rule, which requires financial institutions to establish a comprehensive information security plan in order to safeguard customers' non-public personal information. The proposed amendments would incorporate more robust cybersecurity protocols, including:

- The definition of a security event will no longer include harm as an element. This means that *any* unauthorized access of customer information would be a security event.
- Explicit requirement for access controls on information systems, so that only authorized individuals can access customer information.
- Required audit trails with time-stamped logs of user access and activities to timely detect and respond to security events.
- Required real-time monitoring of user activity to detect abnormal activity from authorized users.
- Limiting retention of customer data that no longer serves a business purpose.
- Testing the effectiveness of access controls with periodic vulnerability assessments.
- Taking inventory of where customer information is saved.

The proposed amendments have been pending for nearly two years and were certainly slowed by COVID-19. It is unknown when the FTC may finalize and implement the proposed amendments to the Safeguards Rule, or indeed whether that will be in 2021. But given the frequency of cyber events during the pandemic and the American public's heightened awareness of these incidents, it's possible the financial industry's landmark piece of privacy legislation may finally be amended this year. Financial institutions should act now by reviewing their existing information security programs in anticipation of the amendments' potential adoption this year.

New Incident Notification Requirements: Proposal Would Require Banks to Move Quickly

The Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB) and the Federal Deposit Insurance Company (FDIC) have issued a notice of proposed rulemaking that would require a banking organization to provide its primary federal regulator with prompt notification of any "computer-security incident" that rises to the level of a "notification incident." The proposal defines a "notification incident" as including cybersecurity incidents that could materially disrupt, impair or degrade their operations, or threaten U.S. financial stability. The proposal would, among other things, require banks to notify their primary regulator of a triggering incident as soon as possible, and no later than 36 hours after learning that the incident occurred, and would require banking service providers to notify affected bank customers immediately after experiencing a security incident that disrupts or impairs services for four hours or more.

If passed in its current form, the proposal would substantially increase the regulatory reporting obligations with which banking organizations must comply. This would be the first substantial update to a bank's responsibility to report a cyber incident in the last 15 years. Indeed, the proposal would subject financial institutions to some of the strictest incident reporting obligations currently in existence in the United States. Banks and banking service providers should continue to follow this proposal and be ready to review and update their incident response plans, business continuity and disaster recovery plans, and vendor management programs to comply with these enhanced requirements.

Cybersecurity Threats Continue to Rise

Last year saw a staggering increase in cyberattacks across multiple industries. On average, an attack occurred every 39 seconds as cybercriminals took advantage of more vulnerable security controls and COVID-19 to compromise companies across the globe. Banks are frequently a prime target for such attacks. In fact, according to a cyber vendor, VMware Carbon Black, attacks on financial institutions spiked by 238% between February and April 2020 alone. Not only are financial service providers a prime target, but according to Accenture and the Ponemon Institute, the cost to address and contain cyber attacks is greater for financial firms than for companies in any other industry – and those costs continue to rise. In particular, ransomware attacks soared exponentially with more sophisticated attacks, higher ransomware demands and layered, persistent threats from cybercriminals. Such attacks are not only extraordinarily burdensome for financial institutions in and of themselves, but they continue to drive up insurance costs for these incidents as well.

The continued attacks against information systems, with a focus on financial institutions, will continue and likely increase in 2021. Cybercriminals are targeting organizations with a low tolerance for business interruption, which includes financial institutions. For example, the Financial Crimes Enforcement Network and the Office of Foreign Assets Control recently issued new advisories on ransomware payments, which has significant impacts on financial institutions. For additional information on these advisories, please see our prior analysis. With remote work likely to continue for the foreseeable future, financial institutions must develop and refine their incident response plans to address these new threats. This also includes testing that plan through a tabletop exercise and evaluating how to respond to such incidents. As the landscape of potential threats continues to grow, financial institutions must be proactive in taking steps to ensure that they are appropriately prepared to respond once an actual attack occurs.

Vendor Management

Vendor management will continue to be a paramount issue for financial institutions this year. New state and industry regulations are imposing stricter requirements upon financial institutions to address cybersecurity risks posed by third-party vendors. These additional requirements come as financial institutions have become increasingly reliant on service providers to provide a variety of essential technology-related products and services. Thus, as cyberattacks continue to evolve, having a strong vendor management program is more critical than ever. This includes reviewing contracts to make sure that appropriate privacy and cybersecurity issues are addressed, updating written policies and procedures regarding the oversight of vendors, and performing risk assessments and due diligence to ensure that vendors have the appropriate controls. Financial institutions should also be evaluating how they would respond if a vendor experiences a cyber incident, as it may involve a variety of factors different from a normal incident. Indeed, vendors should be included in tabletop exercises to ensure financial institutions are ready to respond to a vendor-related security incident.

NYDFS Cybersecurity Regulation

Financial institutions that are subject to the New York Department of Financial Services' (NYDFS) Cybersecurity Regulation already know it is the most comprehensive privacy and cybersecurity regulation focused on the financial industry. Last year, the NYDFS filed its first enforcement action alleging multiple violations of the Cybersecurity Regulation. For more information on this action, see our prior analysis. This year, the NYDFS has already required regulated entities to formally notify the NYDFS if they were directly impacted by the SolarWinds incident. The directive marks yet another unprecedented move by the NYDFS.

It is anticipated that the NYDFS will continue with new enforcement actions this year. Therefore, if your financial institution is a regulated entity with the NYDFS, it is imperative that you have a comprehensive program in place to address the requirements of the Cybersecurity Regulation, including appropriate security controls, a well-established incident response plan, and proper oversight of third-party vendors and service providers.

If you have any questions concerning these issues, or any other aspect of your cybersecurity or privacy programs, please contact the authors or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.