Professional Perspective

Managing Data Compliance Risk to Financial Institutions

Karen Lee Lust, Terrence Vales, and Courtney Fisher, Reed Smith

Bloomberg Law

Read Professional Perspectives | Become a Contributor

Reproduced with permission. Published June 2021. Copyright © 2021 The Bureau of National Affairs, Inc.
800.372.1033. For further use, please contact permissions@bloombergindustry.com

Managing Data Compliance Risk to Financial Institutions

Contributed by Karen Lee Lust, Terrence Vales, and Courtney Fisher, Reed Smith

In the evolving landscape of data privacy compliance, financial organizations must understand the increasingly heightened standards of data governance being enforced by regulatory authorities. Specifically, the Office of the Comptroller of Currency (OCC) has taken a stricter stance on the data security models and policies of financial institutions. In particular, that office is mandating stricter requirements and controls around data and information governance, and more effective technical and organizational safeguards against potential breaches.

In late 2020, a number of globally recognized financial institutions were fined by the OCC in various consent orders for improper handling of information assets. The fines were based on long-established regulations and guidance, but previously not relied on grounds for enforcement actions. These fines were unprecedented in their severity and frequency.

Accordingly, financial institutions should be aware of the pertinent regulations, and how to comply with them through incorporation of best practices around information governance—particularly of consumer personal information.

OCC & Regulatory Mandates

Under 12 C.F.R. Part 30, Appendix D of the OCC Guidelines, the OCC sets forth standards that banks must follow that relate not only to credit and liquidity risk, but also operational and compliance risks. The risks associated with not following these guidelines are two-fold: banks may be fined for not handling data properly, and banks may be fined for not putting in place an effective process for storing, retaining, and timely deletion of excess data for which there is no other legal, regulatory, or business need to retain.

One financial institution was fined $400 million late in 2020 for improper data governance, faulty compliance risk management, and lax internal controls over their data retention procedures. The consent order found that the institution failed to execute a comprehensive plan to address their data governance deficiencies by not establishing independent risk management and inadequately reporting qualitative data governance errors to its board. The OCC mandates that financial institutions create boards of directors tasked with ensuring the institution takes prudent steps in securing data and establishing a written risk governance framework.

The framework must be designed by an independent risk management entity. As boards hold authority over which independent entity creates their risk governance framework, the financial institution bears the liability in using an entity that does not meet OCC standards. Boards of directors should have requisite knowledge of a financial institution's qualitative data governance issues to establish a sufficient risk appetite statement that describes the risk culture associated with the bank. Boards also use this information to impose quantitative limits, using sound stress tests to address data surrounding the bank's earnings, capital, and liquidity.

Improving Data Compliance

Anti-money laundering laws, broker-dealer rules, FINRA, and CFTC requirements for investor communications are just a few laws that apply to financial institutions' retention practices. As a result, the application of retention rules across regulatory requirements and business needs is complex. Financial institutions, like many other established companies, have often kept large volumes of data created in the course of business, while the cost of data storage has decreased.

However, there are other costs inherent in over-retention of information, including the potential for data breaches, litigation/discovery costs that apply once a legal matter is anticipated, and the increasing cost of answering data subject access requests (DSARs) based on personal data privacy laws. While it has been a best practice to remediate or dispose of data that is no longer needed for any business, regulatory, or legal purposes, it is now increasingly an affirmative duty when the information contained includes personal information.

Inventorying Data Assets

It can be a complex undertaking to sift through the various systems and data in a large organization when it is held in so many places, duplicated, and backed up, often more than once. Many organizations feel the pinch of being in between a

©2021 The Bureau of National Affairs, Inc.

rock and a hard place: They must retain what they need to by law and for business purposes, and yet they must ensure they retain no more than that, particularly where the excess information contains personal data.

The patchwork of various regulatory requirements that may apply depending on the nature of the data make it difficult to parse through, identify, and remediate aged data. It's particularly difficult where the origin or nature of the data has become unclear through time—e.g., from an acquisition of a business line, or in a database linked to retired software in backup media. However, the OCC requires institutions to maintain inventories of where customer data resides. Without such an inventory, it would also be difficult to respond to DSARs in a timely way, or be able to properly respond to and assess any damage caused by a data breach.

Financial institutions that properly inventory and track where their most sensitive and highest risk data resides are well-positioned for compliance. In this way, entities can ensure the correct security and access controls are applied where appropriate, and that obsolete data is properly and timely remediated.

Vendor Oversight

Even where an institution has determined it can defensibly dispose of certain data sets, it must go about this disposal process with care by assessing and documenting the risks and the justification for doing so. When engaging vendors to assist, the OCC requires appropriate due diligence and oversight of their work. Late last year, the OCC assessed $60 million in penalties against one institution due to improper oversight of a vendor engaged to decommission two data centers. The OCC found a failure to properly assess the risks of decommissioning the hardware and failure to assess the risk of subcontracting the decommissioning work itself. Relatedly, the institution was found to lack adequate due diligence in the hiring of the vendor, and vendor management control deficiencies which constituted unsafe or unsound practices.

Financial institutions should be mindful of any third-party vendor's own data policies as those frameworks may also be reviewed by the OCC and other regulatory entities. Vendors must ensure that their audit policies comply with regulatory and industry guidelines and are updated to reflect the changes in internal and external risk factors.

Data Security Mandates & Data Migration

For data that is retained, financial institutions are held to a high standard of data security to protect their information pursuant to various standards, including the Gramm-Leach-Bliley Act. According to 12 C.F.R. Part 30, Appendix B, of the OCC Interagency Guidelines, national banks are to implement comprehensive written information security programs that are appropriately scaled to the size of the bank and the scope of its activities. The OCC, jointly with the Federal Deposit Insurance Corporation (FDIC) issued a statement in 2020 to emphasize that supervised financial institutions must apply sound cybersecurity risk management principles to mitigate the risk of a successful cyberattack. This includes effective business continuity planning processes to recover from a disruptive attack, and audits and testing of such data security frameworks.

It is particularly important to ensure data security and integrity is addressed while migrating data –whether for upgrading platforms or moving data to the cloud. A recent OCC consent order focused on a failure to establish appropriate risk management for a transition to the cloud, including a failure to design and implement sufficient network security controls and data loss prevention controls. Prior to any migration, plan in advance with the stakeholders—e.g., from IT, legal, records management, etc.—to solve for a variety of business and legal risks. Data integrity testing, a documented chain of custody for the migration, and procedures for decommission of older systems are also necessary.

Audits Improve Policy Implementation

Internal audits prove helpful in ensuring that data security polices enacted by financial institutions are both properly facilitated and efficient. Moreover, the OCC mandates financial institutions have internal audit functionalities. Such audit plans collect a complete inventory of all the bank's processes, product lines, services, functions, and risk assessments and should be reviewed periodically. Financial institutions must be ready to produce evidence of such compliance materials if their practices fall under regulatory scrutiny.

While financial institutions may commission audits internally, they may also hire external third-party vendors to conduct the audits. Third-party audit vendors not only aid in financial institution risk assessments, but they can also identify weak areas within a bank's data security framework and assist in remediating gaps. Third-party audit services should have capacities that fall in line with the mandates instructed by the OCC. This includes ensuring that audit findings are appropriately

©2021 The Bureau of National Affairs, Inc.

reported on to the board of directors, such that any gaps and weaknesses are raised and addressed. One of the recent OCC consent decrees noted that while one institution had an internal audit function, it was ineffective in identifying numerous weakness and gaps, and also did not effectively report on its findings to be addressed. For the concerns that were raised, the board did not take action to hold the institution's management accountable, which contributed to the finding of unsafe or unsound practices.

Conclusion

As states continue to propose and enact consumer data protection laws and the volume of personal data grows exponentially, the OCC is increasingly holding financial institutions to a high standard through enforcement actions. Accordingly, companies should look to the requirements outlined by the OCC and other regulators to create a comprehensive plan for data risk management and data governance moving forward—and to effectively implement and audit against it.

©2021 The Bureau of National Affairs, Inc.