POLSINELLI | What a law firm should be.™

It's Not Your Fault, but It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks

For organizations that watched (or worse, lived through) the fallout from recent large-scale vendor incidents, the prospect of learning that a trusted vendor has experienced a data incident is almost as distressing as the idea of the organization experiencing an incident itself.

That's because a vendor incident – meaning an incident that occurs at or is otherwise caused by a third-party service provider – can be nearly as time-consuming, costly and reputationally damaging as an internal incident.

Challenges of Vendor Incidents

Vendor incidents can come with all the usual challenges of any security event – operational disruptions, public relations pressures and concerns about data compromise – but often come with the added element of being "in the dark" until a vendor decides to share details about what happened and what they're doing about it. Additionally, depending on the vendor's level of cooperation, the ultimate responsibility to notify individuals may land on the company, even though it is not at fault. All the while, an individual who learned that their data may have been compromised will likely point the finger back at whomever they entrusted their data to, regardless of whether that company is truly where the breach occurred.

Increasing Regulatory Attention

Regulatory bodies, particularly those in the financial industry, are increasingly taking note of this type of incident and raising the level of attention they pay to vendor management. Questions that often come after a company notifies regulators of a vendor incident include: What level of diligence did your organization conduct before trusting a vendor with data? If the vendor made security-related promises – such as to delete data after contract termination – did your organization confirm those promises were kept? Why was a vendor holding so much data for so long?

In 2023, we saw regulatory efforts to gain more insight into these relationships and the risks they pose in the National Credit Union Administration's ("NCUA") approval of a final rule that requires a federally insured credit union to report "reportable cyber incidents" to the NCUA as soon as possible, and in no event later than 72 hours after the credit union reasonably believes that it has experienced a reportable cyber incident.[i] Under the rule, the NCUA suggests that if a *third party* reports experiencing a breach of a credit union's sensitive member information, that credit union likely needs to report the incident to NCUA.[ii] Credit unions have apparently heeded that advice. According to NCUA Chairman Todd M. Harper, "[i]n the first 30 days

after the rule became effective, the NCUA received 146 incident reports, more than it had received in total in the previous year. More than 60 percent of these incident reports involve third-party service providers and credit union service organizations."[iii]

Regulators overseeing banks have so far approached the issue from a slightly different and less direct direction but with a similar result. In guidance issued June 6, 2023, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System and the Office of the Comptroller of the Currency (the "Banking Agencies") provided detailed guidance to banking organizations on vendor management throughout the life cycle of a vendor relationship. This guidance included oversight and accountability procedures for the life of the relationship.[iv] This guidance added to an existing rule issued from the Banking Agencies which requires bank *service providers* to notify bank customers as soon as possible upon experiencing certain types of incidents.

Looking Ahead

Looking ahead to 2024, we can expect continued vendor incident scrutiny on both vendors and the organizations they serve. For its part, the NCUA is currently seeking congressional authority to directly examine third-party vendors, which it cannot do under existing law.

In testimony before Congress, the NCUA has stated that its inability to directly regulate credit union providers "creates a regulatory blind spot"[v] and that without this power, "NCUA is unable to effectively protect credit unions and their members."[vi] If Congress agrees, the NCUA may be given authority to demand information from vendors or impose corrective action plans on them, which vendors can largely ignore under current law.

Given the frequency with which vendor incidents are occurring and the increased regulatory interest in them, organizations should think through what they can do to position themselves for a strong response. For instance, consider: If a regulator inquired about how we vetted a vendor, are we comfortable with our answer? Is our vendor management program robust?

For those on the vendor side of the coin, the challenges are similar, but the key questions are different. Here, consider: if customers impose additional security vetting, are we prepared to provide the accurate and digestible information they'll need to feel comfortable partnering with us?

In all cases, as we head further into 2024, increasing regulatory attention to vendor security should be top of mind.

---

[i] 12 CFR § 748.1(c).
[ii] *See* Appendix A: Examples of Substantial Incidents that Likely Would Qualify as Reportable Cyber Incidents, available at **https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/cyber-incident-notification-requirements/appendix-a**.
[iii] *See* testimony of NCUA Chairman Todd M. Harper Before the Senate Banking, Housing, and Urban Affairs Committee, available at https://ncua.gov/newsroom/testimony/2023/ncua-chairman-todd-m-harpers-written-testimony-senate-banking-housing-and-urban-affairs-committee#:~:text=In%20the%20first%2030%20days,union%20service%20organizations%20(CUSOs).
[iv] *See* Interagency Guidance on Third-Party Relationships: Risk Management, available at **https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf**.
[v] *See* testimony of NCUA Director of Office of Financial Technology and Access Charles A. Vice before the Subcommittee on Digital Assets, Financial Technology and Inclusion.
[vi] Harper testimony, *supra* note 3.