When Your Vendor's Breach Becomes Your Lawsuit: Privacy Risk Lessons from Recent Bank Litigation

May 06, 2026

Categories:

Banking On It
Publications

Authors:

Nancy Eff Presnell
Gene F. Price
Matthew R. Schantz

A recent high-profile incident illustrates the growing litigation and regulatory risks that financial institutions face from vendor-driven data breaches. Within weeks of a national bank confirming a data security incident at a third-party service provider, at least two putative class actions were filed, though none of the alleged conduct appears to have occurred within the bank itself. According to public reporting, the intrusion took place at a third-party vendor; yet the bank, not the vendor, is now defending negligence, breach of fiduciary duty, breach of implied contract, and unjust enrichment claims on behalf of a putative nationwide class.

The bank matter is the latest — but likely not the last — reminder that, from a cybersecurity and litigation standpoint, a financial institution's perimeter is not where its servers end; rather, it extends to wherever its data resides. For bank general counsel (GCs), chief technology officers (CTOs), chief information officers (CIOs), chief information security officers (CISOs), and compliance officers (COs), this litigation validates three distinct but interlocking risks worth re-examining: (1) vendor risk management, (2) litigation exposure under evolving theories of liability, and (3) regulatory compliance with the Interagency Guidelines Establishing Information Security Standards ("Guidelines")[1] issued under the Gramm-Leach-Bliley Act (GLBA), plus the rapidly expanding patchwork of state data security and consumer privacy laws.

The Fact Pattern Banks Should Recognize

The publicly reported allegations follow a familiar pattern. A threat actor compromises a service provider that processes or stores customer data on the bank's behalf. The bank itself is not compromised, but its customers' non-public personal information (NPI) — names, addresses, account numbers, Social Security numbers, drivers' license numbers, and dates of birth — is

exfiltrated.[2] The bank investigates, notifies regulators and affected customers under the Guidelines and applicable state breach notification statutes, and within days finds itself the named defendant in a class action seeking millions of dollars in damages.

The plaintiffs' theory, in broad strokes, is straightforward: the bank owed a duty of care to safeguard customer information; that duty extended to the selection, oversight, and ongoing monitoring of any third party entrusted with that information; and the bank's failure to ensure adequate vendor security caused foreseeable harm in the form of identity theft risk, mitigation costs, and loss of privacy. Whether those theories survive Rule 12(b)(6) motions and whether plaintiffs can establish concrete Article III injury will be litigated. But the cost, distraction, and reputational impact are certain and begin the moment the complaint is filed.

This is not an isolated action. Other recent vendor-driven incidents involving large institutions have produced similar litigation footprints, and some plaintiffs' firms have grown more sophisticated in framing breach-of-fiduciary-duty and implied-contract theories in terms that can survive early dismissal motions even where statutory privacy claims falter.

Risk One: Vendor Management Has Become a Litigation Battleground

Vendor risk management has long been regarded as a regulatory exercise, a function rooted in OCC Bulletin 2013-29 (now subsumed into the 2023 Interagency Guidance on Third-Party Relationships), FDIC FIL-29-2023, and the Federal Reserve's SR Letter 23-4. Banks built vendor inventories, tiered providers by risk, conducted due diligence, and documented oversight. That work remains essential. What has changed is that the same documentation can now serve as the evidentiary backbone of plaintiffs' negligence claims. In a typical class-action breach claim, the bank's contracts, due diligence files, ongoing monitoring records, and incident response logs become exhibits. Using the bank's stated compliance with regulations, plaintiffs can argue:

- The bank knew or should have known about the vendor's security posture based on prior incidents, SOC 2 findings, or industry warnings.
- Boilerplate terms were used in vendor agreements rather than tailored contractual safeguards appropriate for the sensitivity of the data shared.
- The bank failed to check, verify, audit, or respond to known vulnerabilities in the vendor's security posture.
- The bank's inaction delayed the incident response and compounded customer harm.

For those responsible for mitigating data security and privacy risks, the practical consequence is that vendor risk programs should be designed and monitored to withstand discovery, not just to satisfy examiners. In practice, that means several things: Contracts should include specific, customized, and measurable security requirements, not generic or vague IT "industry standard" language. Due diligence should be refreshed on a defined cadence, not simply at onboarding. Findings from SOC 2 Type II audit reports, penetration tests, and the vendor's incident history should be documented, escalated, and acted upon, with any action (or reasoned decision not to act) memorialized. Right-to-audit clauses should be exercised, particularly on high-risk vendors, with a frequency and depth appropriate for the sensitivity of the data. Termination rights tied to security failures should be real rather than theoretical and should be exercised when needed.

Equally important, the bank's incident response plan must explicitly contemplate vendor-driven events. But once such an event occurs, you must know the lay of the land: Who has the authority to demand forensic access? Which contractual mechanisms compel vendor cooperation? How quickly can the bank obtain the data necessary to make accurate and meaningful notification decisions? When a breach occurs, the answers to those questions will determine whether the bank is a sitting duck for litigation or a proactive institution prepared to defend its customers and its interests.

FBT Gibbons

Risk Two: Litigation Theories Are Expanding Faster Than Statutory Defenses

The second risk worth focusing on is the trajectory of plaintiffs' theories. Federal privacy statutes, including GLBA, the Fair Credit Reporting Act, and the Right to Financial Privacy Act, may provide private rights of action for data security failures, but only in narrow circumstances. For a long time, that gap worked in the bank's favor. That is now decreasingly so.

Some plaintiffs' firms are pleading common-law theories that do not depend on a federal privacy statute at all: negligence, negligence per se (predicated on state's Unfair, Deceptive and Abusive Practices (UDAP) statutes or breach notification laws), breach of implied contract, breach of fiduciary duty, and unjust enrichment. They are also leaning heavily on state consumer protection statutes, many of which authorize statutory damages, attorneys' fees, or both. The result is that even where federal preemption arguments and statutory dismissal motions succeed, common-law and state-law claims may survive and drive a pricier settlement.

Risk Three: The Regulatory Floor Is Rising

Even as private litigation expands, the regulatory floor for vendor data security continues to rise. The Guidelines require a covered financial institution to implement written information security programs that designate qualified individuals; mandate risk assessments and access controls (think complex passwords, multi-factor authentication, and more); and require encryption of customers' personally identifiable information (PII) at rest and in transit, secure development practices, monitoring and audits, incident response plans tested in tabletop exercises, and reporting to the board.

Layered on top of that are state legal regimes that no longer reflexively exempt financial institutions. Some states' comprehensive privacy laws have narrowed or eliminated entity-level GLBA exemptions in favor of data-level exemptions, with the result that bank customer data falling outside GLBA's narrow definitions (such as employee data, marketing data, and certain

commercial relationships) is now squarely within the scope of state law. The New York Department of Financial Services' Part 500 regime continues to be a leading example of prescriptive cybersecurity regulation, including for third-party service providers. Massachusetts also has its own long-standing data security regulation, 201 CMR 17.00, with vendor oversight obligations baked in.

As a result, a breach affecting customers in 20 states implicates 20 potential notification regimes, several of which now carry penalty exposure for delayed notification or insufficient detail. This is the new operational reality: a single vendor incident produces a cascade of state attorney general filings, regulator inquiries, and parallel civil litigation.

What Bank GCs, ISOs and COs Should Do This Quarter

Recent vendor-driven incidents do not require a wholesale rebuild of any well-run cybersecurity program. Nonetheless, they justify a focused review of the pressure points where vendor risk, litigation exposure, and regulatory compliance intersect. Financial institutions would do well to reappraise their ability to respond quickly and effectively. Recommended next steps are as follows:

- Re-examine vendors that have access to customer NPI and PII, re-tier them based on actual data sensitivity and volume, and avoid relying on legacy categorizations.
- Audit current vendor contracts for substantive (not boilerplate) security obligations, audit rights, and breach notification timeframes to ensure they meet your most stringent applicable state laws, indemnification, and minimum cyber insurance requirements.
- Pressure-test the incident response plan against a vendor-centric scenario, conducting tabletop exercises with vendors wherever possible. If a current contractual agreement does not allow that level of cooperative preparation, update vendor standards or policies to achieve it on renewals.

- Review customer-facing privacy and security representations in privacy notices, account agreements, websites, and marketing materials, checking for statements that could form the basis of an implied contract or fiduciary duty theory, and align them with actual practices.
- Report to the board regarding vendor cybersecurity risk so that when a vendor incident occurs, the documentary record reflects active oversight rather than detachment or indifference.

None of these steps will completely eliminate the risk of a vendor-driven breach. They will, however, materially improve the institution's posture if and when a complaint is filed. FBT Gibbons works closely with financial institutions to navigate these evolving risks and is available to assist with compliance, incident response preparedness, and vendor risk management. For more information, please contact the authors or any member of FBT Gibbons' Data Security & Privacy or Regional & Community Banks teams.

---

[1] Interagency Guidelines Establishing Information Security Standards, issued jointly by the OCC (12 C.F.R. Part 30, Appendix B), Federal Reserve Board (12 C.F.R. Part 208, Appendix D-2 and 12 C.F.R. Part 225, Appendix F), and FDIC (12 C.F.R. Part 364, Appendix B).

[2] Per 12 CFR § 1016.3(p)(1), "Nonpublic personal information means: **(i)** Personally identifiable financial information; and **(ii)** Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available."

FBT Gibbons