

JUNE 29, 2026 | PUBLICATION

Client Alert: 10 Tips for Managing Third-Party Data Sharing in Financial Services

Key Takeaway: Financial institutions sharing data with third parties face a complex and evolving web of legal obligations. These 10 practical steps can help manage risk across the entire vendor lifecycle.

INDUSTRY SECTOR

Financial Services
Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

Elizabeth R. Brusa

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Financial services businesses routinely share sensitive consumer and business data with third parties across a wide range of functions, including cloud-based banking platforms, artificial intelligence (AI)-powered fraud detection and credit scoring, open banking integrations, outsourced customer service, and more. While these functions are often necessary, each introduces legal, regulatory, and reputational risk that requires deliberate management.

The regulatory landscape has never been more complex. Federal and state privacy laws, prudential banking regulations, cybersecurity mandates, and sector-specific rules like the Gramm-Leach-Bliley Act (GLBA) impose overlapping obligations on financial services companies. While these functions may be outsourced, the liability remains with the financial institution.

The following 10 tips offer practical guidance for building a proactive data-sharing strategy.

1. Know Exactly What Data You Are Sharing, and Share Only What Is Necessary

Before entering any third-party data-sharing arrangement, conduct a thorough data mapping exercise. Maintain a precise inventory of the categories of information to be disclosed, including personally identifiable information, financial account data, transaction histories, and any nonpublic personal information as defined by the Gramm-Leach-Bliley Act (GLBA). Wherever possible, share aggregated or de-identified data to lower breach risk. Document the business purpose for each data element shared. Regulators, and in the event of litigation, opposing counsel, will closely examine whether the scope of data shared was proportionate to the legitimate business need. A disciplined approach to data minimization reduces your exposure to security incidents and unauthorized access, limits regulatory risk, and demonstrates good faith.

2. Conduct Meaningful Vendor Due Diligence

Vendor due diligence should go well beyond a checklist exercise. Before onboarding any third party that will

receive sensitive data, evaluate the vendor's information security posture, privacy compliance program, financial stability, and regulatory track record. Request SOC 2 Type II reports (independent audits of a vendor's security and operational controls), penetration testing results (simulated cyberattacks to identify vulnerabilities), and evidence of compliance with the GLBA and the Federal Trade Commission's Safeguards Rule, which requires covered financial institutions to develop, implement, and maintain a written, comprehensive information security program. Assess whether the vendor has experienced prior data breaches and how they were handled. For vendors interacting with consumer data, confirm appropriate policies around data retention, access controls, and employee training. The depth of diligence should be proportionate to the sensitivity and volume of data involved. For instance, a marketing analytics provider receiving de-identified data warrants different scrutiny than a loan servicer with access to full consumer credit files.

3. Build Robust Contractual Protections

A well-negotiated contract is the backbone of any responsible data-sharing relationship. At a minimum, agreements should include:

- Clearly defined permitted uses and data restrictions
- Confidentiality and data security obligations with specific technical standards
- Mandatory breach notification provisions with defined timelines
- Audit and inspection rights
- Indemnification provisions allocating liability for data incidents
- Restrictions on subcontractors or downstream sharing without prior written consent
- Defined contingency plans and termination strategy that ensures shared data is securely returned or destroyed when the relationship ends, including provisions to revoke the vendor's data use upon a customer's withdrawal of consent. Avoid relying on a vendor's template agreement without substantial negotiation as regulators expect financial services institutions to exercise genuine contractual oversight.

For open banking arrangements subject to Part 1033, contracts should also address authorization disclosures, limits on collection, use, and retention, consumer revocation, restrictions on targeted advertising, cross-selling, and sale of covered data, data aggregator certifications, downstream flow-down obligations, and retention of records evidencing compliance.

4. Address AI and Automated Decision-Making Head On

As AI and machine learning tools become embedded in third-party platforms—from underwriting models and chatbots to fraud scoring and customer segmentation—financial services businesses must account for the unique risks these technologies introduce.

When a vendor uses AI to process your data, understand what data the model was trained on, how automated decisions are made and whether they can be explained, and what steps the vendor takes to test for bias or discriminatory outcomes.

Contractual provisions should ensure that AI model training using customer data complies with applicable laws, including the GLBA, the General Data Protection Regulation (GDPR), Office of the Comptroller of the Currency (OCC) and Federal Deposit Insurance Corporation (FDIC) regulations, Financial Industry Regulatory Authority (FINRA) rules, and state privacy laws. Contracts should address model governance, prohibit use of client data for the vendor's independent model training without consent, require transparency around material algorithm changes, and address ownership of AI-generated outputs derived from shared data.

5. Stay Current with the Evolving Patchwork of Privacy Laws

The U.S. privacy landscape is shifting rapidly. While the GLBA remains the primary federal framework governing financial institutions' handling of consumer data, more than 20 states have enacted comprehensive consumer privacy statutes that regulate the collection, use, sale, and sharing of personal data. Many such state laws include specific provisions around data processing agreements, consumer opt-out rights, and data protection assessments (formal evaluations of privacy risks associated with high-risk data processing activities, such as profiling or targeted advertising) for high-risk processing.

Financial institutions should not assume that GLBA exemptions contained in certain state laws provide blanket coverage for all data-sharing activities, because those exemptions vary by state and often apply only to specific data categories or processing types. Financial institutions must maintain a current, jurisdiction-by-jurisdiction understanding of applicable obligations and ensure their third-party contracts reflect them.

6. Take Open Banking and API-Based Sharing Seriously

Open banking and the proliferation of application programming interfaces (APIs) have fundamentally changed how financial data moves between institutions and third parties. Consumer-authorized data sharing through fintech platforms, account aggregators, and personal financial management tools create consumer value but introduce new privacy, security, and liability considerations.

What the rule does. The Consumer Financial Protection Bureau's (CFPB) Personal Financial Data Rights Rule in Section 1033 of the Dodd-Frank Act establishes a formal framework for consumer-authorized data access. In plain terms, this rule requires financial institutions to make consumer financial data available to consumers and their authorized third parties in a standardized, secure format—giving consumers more control over their own data. The rule sets specific technical, security, and compliance standards for both data providers and authorized third parties. Covered data can include transaction information, account balances, payment-initiation information, account terms and conditions, upcoming bill information, and basic account-verification information, subject to specified exceptions, codified at 12 C.F.R. Part 1033, implements Section Consumer Financial Protection Act and practical covered data providers must make covered data in their control or possession, upon request.

What businesses should do now. Data providers should inventory the data fields they maintain, identify any data excluded under the rule's exceptions, and assess whether their consumer and developer interfaces can deliver covered data in a standardized, machine-readable format. They should also review whether their application programming interface (API) performance, documentation, access controls, security program, denial procedures, revocation mechanisms, and record-retention practices are capable of satisfying Part 1033 if and when applicable compliance obligations take effect.

Pay particular attention to authorized third parties. Third parties seeking access on a consumer's behalf must provide a clear, conspicuous authorization disclosure, obtain the consumer's express informed consent, limit collection, use, and retention to what is reasonably necessary to provide the consumer-requested product or service, and provide a revocation method that is as easy to access and operate as the initial authorization. The rule also restricts treating targeted advertising, cross-selling, or sale of covered data as reasonably necessary to provide the requested product or service and requires certain downstream recipients and data aggregators to accept comparable obligations. Although the rule's compliance dates are currently stayed, financial services businesses should proactively assess their API security protocols, implement strong authentication and authorization controls, and ensure consumer consent mechanisms are transparent, revocable, and well-documented.

7. Plan for Data Breaches Before They Happen

Breach notification laws now exist in all 50 states and continue to be amended with shorter notification windows and expanded definitions of covered data. When a third-party vendor suffers a data breach involving your customers' information, your organization will typically bear the regulatory and reputational consequences.

Implement stringent security and encryption controls when storing or sharing sensitive data across networks and consider requiring multi-factor authentication for anyone accessing your data environments. Ensure your incident response plan specifically addresses third-party breach scenarios, including escalation protocols, communication templates, regulatory notification procedures, and defined roles.

Contracts should require vendors to notify you of any suspected or confirmed incident within 24 to 48 hours and to cooperate fully with your investigation. Conduct tabletop exercises simulating a third-party breach to test readiness and revisit your response plan regularly.

8. Monitor Third-Party Relationships on an Ongoing Basis

Due diligence should not end at onboarding. Regulatory guidance from the OCC, the Federal Reserve, the FDIC, the CFPB, and state regulators consistently emphasizes that financial institutions must conduct ongoing monitoring commensurate with the risk and complexity of each arrangement.

This includes periodic reassessment of vendor security controls, review of updated audit reports and certifications, monitoring of the vendor's financial condition, and tracking of regulatory actions or security incidents. Establish a formal review cadence and document findings.

If a vendor's risk profile materially changes such as through a merger, a significant security incident, or a change in subcontracting arrangements, your organization should respond swiftly by exercising contractual audit rights or terminating the relationship if necessary.

9. Do Not Overlook Downstream and Fourth-Party Risk

One of the most underestimated risks in third-party data sharing is the potential for your data to be further shared by your vendor with its own subcontractors, cloud providers, or other downstream recipients, sometimes called fourth parties. Each additional link in the chain introduces new vulnerabilities and reduces your visibility into how data is handled. Contracts should require vendors to disclose subcontractors that will access your data and to flow down equivalent data protection obligations. Where feasible, require prior written approval before a vendor engages a new subcontractor. In cloud-based models, your data may be processed across multiple environments and jurisdictions. Ensure your contractual and compliance frameworks account for this complexity.

10. Foster a Culture of Accountability, Not Just Compliance

The most effective third-party data governance programs are built on a culture that treats data stewardship as a core business value, not solely on contracts and checklists. This means investing in regular training for employees who manage vendor relationships, integrating third-party risk management into enterprise-wide risk frameworks rather than siloing it in a single department, and ensuring senior leadership and board-level committees receive meaningful reporting on third-party data risks. It also means approaching vendor oversight as a collaborative process. Vendors that understand your expectations and share your commitment to data protection are far more likely to perform well than those simply bound by contractual language. Building genuine partnerships around data governance while maintaining the controls necessary

to protect your institution and customers is the hallmark of a mature program.

The volume and variety of data flowing between financial services businesses and their third-party partners will only continue to grow, as will regulatory expectations and enforcement activity. Institutions that invest now in rigorous data governance, thoughtful contracts, ongoing monitoring, and a genuine culture of accountability will be far better positioned to capture the benefits of third-party innovation while managing the accompanying risks. The cost of getting this right is significant, but it pales in comparison to the financial, regulatory, and reputational cost of getting it wrong.

For questions about third-party data sharing, vendor risk management, or financial services privacy compliance, please contact Elizabeth R. Brusa or Jeff M. Smith in Shumaker's Financial Services practice group.