THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 41 No. x x 2025

**PRE-PUBLICATION ISSUE**

# EXAMINING HOW EXISTING FEDERAL CONSUMER PRIVACY LAWS APPLY TO THE OPEN BANKING ECOSYSTEM

*This article examines how existing federal consumer financial privacy laws in the United States, namely the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, apply to the open banking ecosystem, particularly in light of the Consumer Financial Protection Bureau's recently promulgated Personal Financial Data Rights rulemaking under Section 1033 of the Dodd-Frank Act. While these new rules require data providers and authorized third parties to implement several new consumer protections, they were crafted to work in conjunction with existing privacy laws. The overlap of these new rules with legacy privacy frameworks is examined to demonstrate how they work in tandem and how they will work going forward if the new rules are vacated through pending litigation. In some cases, the new rules introduce stricter limitations on the access, use, retention, and redisclosure of data than existing federal consumer financial privacy laws, raising complex operational questions for entities involved in the open banking ecosystem.*

By Adam Maarec *

The Consumer Financial Protection Bureau ("CFPB") finalized its Personal Financial Data Rights rulemaking (the "Final Rule") under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act") in November 2024.[1] But after two national banking trade associations filed suit to block the Final Rule from taking effect, and the CFPB joined the banks in asking the court to vacate its own rules, companies operating in the open banking market are left with uncertainty regarding the rules that apply to their activities.

Companies sharing and accessing customers' sensitive financial account data need to consider how existing consumer financial protection laws might apply to their open banking activities — with or without the Final Rule. Open banking generally refers to consumer-authorized data sharing. For example, when a consumer authorizes a third party to access and directs their bank to electronically share deposit account or credit card data (in many cases via a data aggregator) what federal consumer financial privacy laws apply?

[1] 89 Fed. Reg. 90838 (November 18, 2024).

* *ADAM MAAREC is a partner in the Financial Institutions Compliance group at McGlinchey Stafford, PLLC in Washington, DC. Advising participants across the banking and fintech ecosystem, Adam represents banks of all sizes, non-bank lenders and bank partners, digital wallet providers, payments processors, and companies offering innovative consumer financial management tools. His email address is amaarec@mcglinchey.com.*

***IN THIS ISSUE***

•

***RSCR Publications LLC*** Published 12 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $650 per year in U.S., Canada, and Mexico; $695 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call (866) 425-1171 or visit our Web site at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail shimmelfarb@comcast.net. To submit a manuscript for publication contact Ms. Himmelfarb.  ISSN: 1051-1741. 

## BUT FIRST, WHAT DATA IS BEING SHARED IN OPEN BANKING USE CASES TODAY?

Open banking use cases involve access to a wide range of data needed to deliver innovative products and services. In the US today, open banking use cases have developed organically to include a broad scope of financial products and services — consumer deposit accounts, credit cards, mortgages, auto loans, student loans, personal loans, buy-now-pay-later products, investment accounts, and retirement accounts — and involve the sharing of detailed account-level information, such as balances, past debits and credits, identity information regarding the account's owners, and many other account details that may be available in a typical online banking experience.

Section 1033 of the Dodd-Frank Act generally requires any "information in the control or possession of [a] covered person concerning [a] consumer financial product or service that the consumer obtained from such covered person" to be made available electronically (subject to a few exceptions).[2] "A consumer financial product or service" is defined in the Dodd-Frank Act to include all of the products listed above, but it does not capture certain accounts that are beyond the CFPB's jurisdiction, such as investment and retirement accounts.

The Final Rule limits the scope of accounts and data required to be disclosed even further.[3] Under the Final Rule, "data providers" are required to make available "covered data" about specific account types, namely deposit accounts and credit cards.[4] The covered data fields required to be disclosed by the Final Rule include:

- *Transaction information*: 24 months of transaction details, including amount, date, payment type, pending or authorized status, payee/merchant name, rewards, credits, and fees or finance charges.
- *Terms and conditions*: agreements evidencing legal obligations, including account opening agreements, pricing information and fee schedules, credit limits, rewards program terms, overdraft coverage status, and arbitration agreement status.
- *Upcoming bill information*: third-party bill payments scheduled through the data provider, e.g., payments scheduled to a utility company using a bank bill pay service, and any upcoming payments due from the consumer to the data provider, e.g., minimum due on a credit card.
- *Account balances*: this can include multiple balances, e.g., a credit card may have a cash advance balance, statement balance, and current balance.
- *Basic account verification information*: name, address, e-mail address, and phone number, and for Reg E and Reg Z accounts directly or indirectly held by the data provider, a truncated account number or other account identifier.
- *Information to initiate payments*: to or from a Reg E account directly or indirectly held by the data provider, including an ACH account number and routing number.[5]

The CFPB noted that the Final Rule applies contemporaneously with existing federal privacy laws, such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. Therefore, data providers should be

[2] 12 U.S.C. 5533(a).

[3] Note that, while the Final Rule limits the scope of accounts and data to be shared, if the rule is vacated such a limitation would no longer exist.

[4] 12 C.F.R. 1033.111(c) (defining a "data provider"), 1033.111(b) (defining a "covered consumer financial product or service" as a consumer financial product or service that is (1) a "Regulation E account"; (2) a "Regulation Z credit card"; or (3) involves the "facilitation of payments from a Regulation E account or Regulation Z credit card."), and 1033.201(a) (requiring a data provider to "make available to a consumer and an authorized third party, upon request, covered data in the data provider's

*footnote continued from previous column…*

control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider, in an electronic form usable by consumers and authorized third parties").

[5] 12 C.F.R. 1033.211.

aware of how data shared in the open banking ecosystem today, and pursuant to the Final Rule in the future should it survive the current legal challenge, will be governed under existing federal privacy laws.

## A BRIEF OVERVIEW OF THE GRAMM-LEACH-BLILEY ACT'S ("GLBA") REQUIREMENTS.

GLBA became law in 1999 and its implementing regulations (Regulation P) govern the handling and sharing of "nonpublic personal information" ("NPI"). NPI is defined by statute as: "personally identifiable financial information: (1) provided by a consumer to a financial institution; (2) resulting from any transaction with the consumer or any service performed for the consumer; or (3) otherwise obtained by the financial institution."[6] GLBA further provides that NPI includes "any list, description, or other grouping of consumers . . . derived using any nonpublic personal information other than publicly available information."[7] A "financial institution" is broadly defined to include "any institution the business of which is engaging in financial activities" as described in the Bank Holding Company Act (Section 1843(k) of Title 12).[8]

GLBA generally prohibits a financial institution from disclosing NPI to non-affiliated third parties unless certain conditions are met.[9] A key exception that enables open banking use cases today appears in Section 15 of Regulation P. This section permits disclosure of NPI to a non-affiliated third party "with the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction."[10]

Under the Final Rule, the CFPB noted that it "does not affect a person's obligations or duties under the GLBA."[11] So, in the event that the rules overlap, *the more restrictive provisions would apply.* For example, the CFPB stated that while "GLBA and Regulation P may permit some uses of information that may not be permitted under the final rule, compliance with the final rule does not require a person to violate the GLBA or Regulation P."[12]

In the context of the Final Rule and the open banking ecosystem more broadly:

- A "data provider" offering a deposit account or credit card under the Final Rule, along with any other bank or non-bank offering other consumer financial products and services whose data will be accessed by third parties in open banking use cases, will ordinarily be considered a "financial institution" under GLBA;

- Nearly all "covered data" under the Final Rule, and all customer-specific personally identifiable data shared in open banking use cases, will be considered NPI subject to GLBA's limitations; and

- Nearly all "authorized third parties" with a right to access covered data under the Final Rule, and other third parties accessing and receiving data in open banking use cases, would be considered non-affiliated third parties receiving NPI (and "financial institutions" depending on the activities they conduct) under GLBA.

## GLBA OBLIGATIONS APPLY TO OPEN BANKING DATA AS NPI.

Assuming that each third party possessing data in open banking use cases is a financial institution in receipt of NPI, GLBA and Regulation P may place limits on the third party's use and disclosure of that data. Importantly, *NPI does not lose its character as NPI when it is disclosed at the direction of the consumer with another financial institution*.

- *Applicability of Safeguards Rules to NPI when held by a data provider*. Sections 501 and 505(b)(2) of GLBA generally direct the federal banking regulatory agencies and the Federal Trade Commission to set standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to

[6] 15 U.S.C. 6809(4)(A).

[7] 15 U.S.C. 6809(4)(C).

[8] 15 U.S.C. 6809(3)(A). The Federal Reserve Board has issued regulations further defining which activities are "financial in nature or incidental to financial activities." 12 C.F.R. 225.86.

[9] 12 C.F.R. 1016.10(a).

[10] 12 C.F.R. 1016.15(a)(1). In open banking data sharing experiences today, a consumer will ordinarily: (1) authorize a third party to access data; (2) then be directed by the third party to the bank; and (3) authorize the bank to share specific data with the third party. NPI could potentially be shared under other exceptions in Regulation P, such as the exception under Section 1016.14(a)(1) that permits sharing in connection with "servicing or processing a financial product or service that a customer requests or authorizes."

[11] Final Rule at 90851.

[12] *Id*.

protect the security, confidentiality, and integrity of customer information. The federal banking agencies first issued interagency guidelines in 2001, titled the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*,[13] and the Federal Trade Commission issued its own iteration shortly thereafter.[14] They are collectively referred to as the Safeguards Rules.[15]

"Customer information" subject to the agencies Safeguards Rules covers "any record containing nonpublic personal information about a customer of a financial institution." So financial institutions holding open banking data regarding consumer financial products and services, including "covered data" under the Final Rule, are generally subject to one iteration or another of the GLBA's Safeguards Rules and have a duty to protect this information. That duty includes protecting against "unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer"[16] and adopting practices that are appropriate for the institution, including "[a]ccess controls on customer information systems, including controls to authenticate and permit access only to authorized individuals."[17]

In short, the Safeguards Rules establish a general obligation for financial institutions to protect information held about the financial products and services they deliver to consumers. When a third party seeks to access that data — whether by screen scraping or by more secure and sanctioned channels, and whether under the broad reach of open banking or the narrower Final Rule — it is incumbent upon the financial institution to evaluate the third party, impose proper authentication protocols, and prevent unauthorized access.

- *Limits on use and redisclosure of NPI*. Regulation P provides for the continued protection of NPI after it is received by non-affiliated third parties that are financial institutions.[18] Relevant to consumer-permissioned sharing in open banking and the Final Rule, Regulation P states that such non-affiliated third parties receiving NPI may only "use and disclose [the NPI received under the exceptions in Section 15] in the ordinary course of business *to carry out the activity covered by the exception under which you received the information*." (Emphasis added).[19] Regulation P also notes in an example that, with respect to a nonaffiliated third party receiving NPI under a Section 15 exception, "you could not disclose that information to a third party for marketing purposes or use that information for your own marketing purposes." In other words, when a financial institution receives NPI from another non-affiliated financial institution "with the consent or at the direction of the consumer" under Section 15 of Regulation P, the financial institution may only use and redisclose that NPI within the scope of the consumer's consent or direction.

  This limitation on use and disclosure is similar to the data minimization principles in the Final Rule, which provide that an authorized third party may only *collect, use, and retain* covered data as "reasonably necessary to provide the consumer's requested product or service."[20] So, while Regulation P limits the disclosure of NPI by a financial institution and the use of data by a recipient (that is also a financial institution) based on the scope of the customer's consent, the Final Rule goes further than Regulation P by: (1) restricting the *access and retention* of data by any authorized third party, versus Regulation P's

[13] Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616 (February 1, 2001).

[14] Standards for Safeguarding Customer Information, 67 FR 36484 (May 23, 2002).

[15] The Safeguards Rules have been updated since they were initially promulgated. *See* the Federal Trade Commission's Safeguards Rule, 16 C.F.R. part 314, and the Interagency Guidelines Establishing Standards for Safety and Soundness, 12 C.F.R. part 30, app. A (OCC); 12 C.F.R. part 208, app. D–1 (Bd. of Governors of the Fed. Rsrv. Sys.); 12 C.F.R. part 364, app. B (FDIC); and 12 C.F.R. 748, app. A (NCUA).

[16] 12 C.F.R. § Pt. 30, App. B, Supp. A (I)(A)(3).

[17] 12 C.F.R. § Pt. 30, App. B, Supp. A (I)(B)(2)(a).

[18] 12 C.F.R. 1016.11(a)(1). Note that the application of GLBA and Regulation P is generally limited to financial institutions. 12 C.F.R. 1016.1(b)(1). As a result, the limitations on use and redisclosure afforded to NPI described here may not apply if the recipient is not a financial institution subject to GLBA and Regulation P.

[19] *Id*. This provision also permits the disclosure of NPI to affiliates of the financial institution from which the information was received and to the recipient's affiliates (though these recipients are subject to the same use and disclosure limitations).

[20] 12 C.F.R. 1033.421(a).

limits on a financial institution's *disclosure* of data and a receiving financial institution's *use and redisclosure* of data and (2) tying the limitations on access, use and retention of covered data by a third party to what is "reasonably necessary" to deliver the customer's requested product or service, versus Regulation P's limits based on the consent or direction of the consumer.

- *Applicability of Safeguards Rules to NPI upon receipt*. The Final Rule requires that an authorized third party agree to protect covered data received from a data provider in accordance with the GLBA's Safeguards Rules, even if the authorized third party may not be considered a "financial institution" under GLBA.[21] With respect to financial institutions, this appears to largely be a statement of existing obligations. As noted above, the GLBA Safeguards Rules require any financial institution holding customer information to: "ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer."[22]

  In other words, the Final Rule's obligation for all authorized third parties to commit to the Safeguards Rule is duplicative in most cases, where financial institutions receiving NPI from an unaffiliate third party are already subject to these obligations. The Final Rule expands coverage to others that might otherwise be beyond the reach or exempted from coverage of the Safeguards Rules, such as entities that "are not significantly engaged in financial activities," like a "retailer [that] merely . . . accepts payments in the form of cash, checks, or credit cards that it did not issue."[23] But the obligation for a financial institution to protect customer information received under the Final Rule — or open banking more broadly — ought to be subject to the Safeguards Rule regardless.

[21] 12 C.F.R. 1033.421(e). See also 89 Fed. Reg. 90944 (discussing how certain entities that are not financial institutions, namely merchants, must certify their adherence to the GLBA Safeguards Rule to become an authorized third party because other data security requirements that may apply (e.g., PCI and Nacha requirements) are not sufficient).

[22] Standards for Safeguarding Customer Information, 67 FR 36484 (May 23, 2002).

[23] 12 C.F.R. 314.2(h)(4)(ii).

## THE FAIR CREDIT REPORTING ACT & OPEN BANKING DATA.

The Fair Credit Reporting Act ("FCRA") generally governs the creation, sale, and use of "consumer reports."[24] A consumer report is "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility" for personal credit or insurance, employment or certain other permissible purposes.[25] A consumer reporting agency is circularly defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in . . . assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[26] The entities that provide data to consumer reporting agencies are generally known as "furnishers," defined under the FCRA's implementing regulation, Regulation V, as "an entity that furnishes information relating to consumers to one or more consumer reporting agencies for inclusion in a consumer report . . . "[27]

While the CFPB concluded that the Final Rule "does not affect a person's obligations or duties under the FCRA"[28] and that a person subject to the FCRA and the Final Rule "must comply with both,"[29] several questions arise regarding the overlap of FCRA with open banking and the Final Rule. For example, are data providers also furnishers of data when they share data with an authorized third party or data aggregator? Under what circumstances might authorized third parties or data aggregators become a consumer reporting agency? And when authorized third parties receive covered data under the Final Rule or open banking more broadly, when is that information subject to FCRA as a consumer report and its limitations on the use and reuse of consumer reports for specific "permissible purposes"?

In addition to acknowledging "that the potential applicability of the FCRA to uses of covered data under

[24] 15 U.S.C. 1681 et seq.

[25] 15 U.S.C. 1681a(d).

[26] 15 U.S.C. 1681a(f).

[27] 12 C.F.R. 1022.41(c).

[28] Final Rule at 90849.

[29] Final Rule at 90850.

the final rule presents operational complexity . . . ,"[30] the CFPB included some helpful guidance in the preamble to the Final Rule.

- *Data providers are not "furnishers."* The CFPB clarified in the preamble to the Final Rule that it "would not consider data providers . . . to be furnishers solely by virtue of permitting data access . . . " even if the data is provided to a data aggregator that may be engaged in activities of a consumer reporting agency.[31] The CFPB's reasoned that "the consumer, and not the data provider, would be the party that is [providing] data to the consumer reporting agency" and thus would not be considered a "furnisher" providing data to a consumer reporting agency on its own volition.

- *Data aggregators could be consumer reporting agencies.* In a separate (and now withdrawn) proposed rule that would have expanded the scope of Regulation V to address "data broker" practices, the CFPB discussed a variety of activities that could be viewed as assembling or evaluating data and cause the entity performing the activities to be considered a "consumer reporting agency" subject to the FCRA.[32] In discussing these activities, the proposed rule stated that "a person assembles or evaluates when the person collects information from a consumer's bank account and assesses it, such as by grouping or categorizing it based on transaction type."[33] The CFPB acknowledged "that data aggregators often engage in such activities . . . [applying their] own taxonomy to group or categorize the collected information. To take just one factual scenario, a data aggregator that collects bank account information pursuant to consumer authorization in connection with a loan application may group or categorize deposits or withdrawals by type of income or expense, such as 'rent' and 'loan repayment,' prior to sharing it with the lender. In doing so, the data aggregator assembles or evaluates the information."[34] On the other hand, however, it remains unclear what data aggregator activities would *not* constitute assembling or evaluating data, such as merely transforming data into a standardized data format.

- *Data from data aggregators could be consumer reports.* The FCRA's definitions of a consumer report and a consumer reporting agency are interdependent. So whether information obtained via open banking or the Final Rule is assembled and evaluated, and then sold to be used (or is expected to be used) as a factor in establishing a consumer's eligibility for personal credit or insurance, employment or certain other permissible purposes, together determines whether the data may be a consumer report and the entity selling the information may be a consumer reporting agency. This is a fact-specific inquiry that must be done under FCRA today, with or without the Final Rule.

FCRA places limits on the "permissible purposes" for which consumer report information can be used. However, those limitations do not include the "reasonably necessary" standard found in the Final Rule. So, in some respects, the Final Rule places greater limitations on the use and sharing of covered data than on consumer reports, and those greater limitations must be applied to covered data when it is part of a consumer report, even if FCRA would otherwise permit such use.

## THE FINAL RULE PLACES SOME LIMITATIONS ON COVERED DATA THAT GO BEYOND GLBA AND FCRA.

Regardless of what terms of use appear in a third-party's terms and conditions or privacy policies, and regardless of the use and disclosure of data that may be permitted (or restricted) under applicable law, uses of covered data by an authorized third party beyond what is "reasonably necessary" to provide the requested product or service are generally prohibited by the Final Rule. In this way, the Final Rule places additional restrictions on the access, use, and retention of financial data above and beyond the restrictions that already exist — and continue to apply — under GLBA and FCRA. The Final Rule states that it is almost always not reasonably necessary, and thus an improper secondary use of data, to engage in targeted advertising, to cross-sell other products or services, or to sell data to third parties.

While data providers may applaud the Final Rule's restrictions on downstream uses of data by third parties, such as using data to build unrelated models or reverse

[30] Final Rule at 90851.

[31] Final Rule at 90850.

[32] Protecting Americans From Harmful Data Broker Practices, 89 Fed. Reg. 101402 (December 13, 2024). Also note that, as of November 2024, the CFPB confirmed that "Supervisory examinations over one or more data aggregators, including larger participants in the consumer reporting market, are scheduled or ongoing . . . " Final Rule at 90852.

[33] 89 Fed. Reg. 101402, 101426 (December 13, 2024).

[34] *Id*.

engineer confidential or proprietary algorithms, recipients of data seeking to use it for innovative-use cases may find themselves constrained and struggle to operationalize controls to ensure their access, use, and retention of data is appropriately limited. In practice, this requires every use of data to be evaluated against the original reason for which it was collected. Moreover, the obligation to only retain data as long as reasonably necessary amounts to an obligation to purge data once retention is no longer necessary, which may also present operational challenges.

## CONCLUDING THOUGHTS ON THE OVERLAPPING PRIVACY REQUIREMENTS APPLICABLE TO OPEN BANKING.

In crafting the Final Rule, the CFPB created new obligations that work in conjunction with existing federal privacy frameworks, particularly those under the GLBA and FCRA. But with or without the Final Rule, companies providing data and accessing data in the open banking ecosystem need to understand how these decades-old laws apply to modern technology and open banking use cases, including limitations on data use and disclosure and data security requirements. ■