ACH Operations Bulletin #3-2024:

Open Banking and ACH Payments:
The Impact of the CFPB's Personal Financial Data Rights Final Rule
October 31, 2024

Executive Summary

On October 22, 2024 the Consumer Financial Protection Bureau ("CFPB") released its final rule implementing section 1033 of the Consumer Financial Protection Act (the "Personal Financial Data Rights Final Rule" or "Final Rule").[1] This ACH Operations Bulletin provides an overview of the Final Rule and an initial assessment of its applicability and impact on ACH Network participants and ACH payments. ACH Network participants should take note, in particular, that:

1. A consumer's authorization to share data as provided for in the Final Rule, including the "information to initiate payment to or from a Regulation E account," is separate and distinct from a consumer's authorization to initiate an ACH payment to credit or debit their account;

2. Receiving Depository Financial Institutions ("RDFIs") must comply with the Final Rule's requirement to make routing and account numbers available through consumer and developer interfaces at no cost;[2] and,

3. The Nacha Operating Rules ("Nacha Rules") apply, and will continue to apply, to all ACH payments, including those for which the routing and account numbers are obtained through open banking methods, just as if the Receiver had provided that information directly to the payment Originator.

The CFPB's Personal Financial Data Rights Rule

On October 22, 2024 the CFPB released the Personal Financial Data Rights Final Rule implementing section 1033 of the Consumer Financial Protection Act and requiring the establishment of an open banking framework. Under the Personal Financial Data Rights Final Rule, data providers, including depository institutions, must make covered data available, at no cost, to consumers and their authorized third parties in a usable electronic form. Data providers

---

[1] *See* CFPB Personal Financial Data Rights Final Rule, https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/. As of this writing, the Final Rule has been challenged in court, so its ultimate implementation remains uncertain.

[2] The court challenge asserts that the CFPB overstepped its statutory authority with respect to including payment information as part of the Final Rule's covered data.

must provide such covered data to consumers and authorized third parties through established consumer and developer interfaces.

In order to receive covered data, authorized third parties must obtain the consumer's express, informed consent through a signed authorization disclosure that is clear and conspicuous and segregated from other materials. Authorized third parties are also subject to a number of obligations related to their data access, including restrictions on data collection, use and retention, satisfaction of information security requirements and the provision of a reasonable method for consumers to revoke the third party's authorization to access their covered data. Compliance dates for the Final Rule are staggered for depository institutions based on asset size, with the largest depository institutions, those holding at least $250 billion in total assets, having until April 1, 2026 (the earliest applicable date) to comply.[3]

Impact of the Personal Financial Data Rights Final Rule on ACH Network Participants and ACH Payments

Nacha understands that some ACH Network participants have questions about the implications of the Final Rule for ACH transactions. First and most importantly, the Final Rule relates to required information sharing by data providers. It does not change any applicable requirements regarding the authorization, origination or processing of ACH transactions. Second, the Nacha Rules continue to provide important guardrails if covered data is used in connection with ACH transactions. Accordingly, this Bulletin is intended to highlight the continued applicability of the Nacha Rules to ACH payments that involve data obtained through the open banking framework.

Applicability of the Personal Financial Data Rights Final Rule to ACH Network Participants

The CFPB's Final Rule solely governs the sharing of consumer data between data providers and authorized third parties and consumers; it does not impose any requirements related to the authorization or processing of consumer ACH transactions. However, ACH Network participants are impacted by the Final Rule due to their status as data providers. Specifically, RDFIs are covered under the Final Rule as data providers of the information needed to initiate a payment to or from a consumer's Regulation E account, i.e. routing and account numbers. As covered data providers, RDFIs must comply with the Final Rule's data sharing and interface establishment requirements. Additionally, the Final Rule requires third parties to obtain a consumer's consent to access data through a clear and conspicuous, segregated authorization. ACH Network participants should keep in mind that "authorized data access, in and of itself, is not payment authorization" and that "product or service providers that access information and initiate payments [must] obtain separate and distinct consumer authorizations for these separate activities."[4]

---

[3] Data providers with assets equal to or less than the Small Business Administration (SBA) size standard are exempt from the Final Rule. The current SBA size standard for commercial banking is $850 million in assets.

[4] *See* CFPB, Consumer Protection Principles: Consumer-Authorized Data Sharing and Aggregation, 4 (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

<u>Applicability of Existing Nacha Rules to Payments Using Information Obtained Through Open Banking</u>

While the ability of authorized third parties to obtain information necessary to initiate ACH transactions pursuant to the Final Rule potentially raises risks for financial institutions involved in such transactions, the Nacha Rules continue to govern the actual authorization, processing and movement of ACH payments. Moreover, the existing Nacha Rules already incorporate various established protections for banks and consumers that will continue to apply under the open banking regime, including with respect to transaction authorization procedures, consumer protection from unauthorized ACH transactions, record retention, data security, sharing of certain ACH data, and risk management.

Authorization Procedures
- With respect to ACH Entries that utilize data obtained via open banking (e.g., routing and account numbers),[5] the Nacha Rules' existing transaction authorization requirements continue to apply. Mere authorization to share data does not constitute authorization to initiate transactions based on that data. The Nacha Rules already require that authorizations for consumer debit Entries be in writing signed or similarly authenticated by the Receiver[6] and be clear and readily understandable.[7] Moreover, the Nacha Rules specifically require that authorizations be obtained by (and revoked with) the payment Originator.[8] The Final Rule is consistent with this requirement by mandating that open banking data authorization disclosures be "clear, conspicuous, and segregated from other material," e.g., a transaction authorization.[9]

Consumer Protection from Unauthorized ACH Transactions
- The Nacha Rules provisions regarding allocation of responsibility for unauthorized ACH Entries apply and will continue to apply to Entries that rely on open banking data. The existing Nacha Rules requirements already provide robust allocation of responsibility to the ODFI, and by extension to the Originator, for unauthorized ACH Entries.[10] Under the

---

[5] The Final Rule permits RDFIs to tokenize account numbers that are provided through the open banking regime. *See* 12 C.F.R. § 1033.211(c)(1). Although the Nacha Rules also permit tokenization of account numbers, tokenization involves a variety of complexities, including the ability to relate transactions involving tokens to underlying accounts for customer service purposes.

[6] Under the Nacha Rules, a Receiver is a Person that has authorized an Originator to initiate a credit Entry, debit Entry, or Non-Monetary Entry to the Receiver's account at the RDFI. With respect to debit Entries, the term "Receiver" means all Persons whose signatures are required to withdraw funds from an account for purposes of the warranty provisions of Subsection 2.4.1 (General ODFI Warranties). *See* Nacha Rules: Section 8.84. For example, a consumer who authorizes the sharing of his/her account number pursuant to the Final Rule, is the "Receiver" of any debit Entry based on that account information and would need to separately authorize the ACH debit to his/her account.

[7] *See* Nacha Rules: Section 2.3.1 (Originator Must Obtain Authorization from Receiver); Section 2.3.2.2 (Debit Entries to Consumer); and Section 2.3.2.5 (Standing Authorization for Debit Entries to Consumer Accounts).

[8] *See* Nacha Rules: Section 2.3.2.2 (Debit Entries to Consumer).

[9] Proposed 12 C.F.R. § 1033.411(a).

[10] *See* Nacha Rules: Section 2.13.2 (ODFI Request for Return); Section 3.7.1 (RDFI Obligation to Stop Payment of Entries to Consumer Accounts); Section 3.12 (Written Statement of Unauthorized Debit (WSUD)); Section 3.12.1 (Unauthorized Debit Entry/Authorization for Debit Has Been Revoked); Section 3.12.4 (Form of Written Statement of Unauthorized Debit); and Section 3.12.5 (Retention of Written Statement of Unauthorized Debit).

Nacha Rules, an RDFI must recredit a consumer for an unauthorized ACH debit if the consumer provides timely notice. The Nacha Rules further allow the RDFI to return such an unauthorized ACH debit to the ODFI within specified timeframes. ODFIs will want to ensure that their Originators that use open banking data are obtaining separate ACH transaction authorizations that meet the standards of the Nacha Rules.

Record Retention
- Although the Final Rule has certain record retention requirements for authorized third parties that obtain covered data, the Nacha Rules' existing record retention requirements related to the authorization and processing of ACH Entries[11] apply and will continue to apply to Entries that rely on open banking data.

Data Security
- Although the Final Rule imposes data security requirements on authorized third parties that obtain consumer data under the open banking framework, the Nacha Rules' existing data security requirements apply and will continue to apply to routing and account numbers used in ACH Entries, regardless of whether this information is obtained through open banking methods. These Nacha Rule provisions already require the secure handling and protection of origination information.[12] It is generally expected that compliance with the Gramm-Leach-Bliley Act "safeguards" requirements referenced in the Final Rule will also satisfy the Nacha Rules' requirements.

Data Sharing by Authorized Third Parties
- The Final Rule limits the purposes for which "authorized third parties" can reshare data gathered via open banking. Consistent with federal law limiting "data passes" to post-transaction third party sellers in internet transactions, and with the goal of protecting consumers against unintended charges against their accounts, the Nacha Rules further already prohibit an ODFI or Originator from disclosing a Receiver's account number or routing number to a third party to originate a separate debit entry.[13] This provision of the Nacha Rules applies to the same extent to information obtained through open banking as it does to information directly entered by a consumer themselves.

Risk Management
- The Nacha Rules already impose general risk management standards on ODFIs that include, among other things, an obligation to assess the nature of an Originator's ACH activities and the risks those activities present.[14] As open banking is implemented, ODFIs

---

[11] *See* Nacha Rules: Section 1.4.1 (Retention Requirement for Records of Entries); Section 1.4.2 (Provision Requirement for Records of Entries); Section 1.4.3 (Electronic Record Creation and Retention); Section 2.3.2.7 (Retention and Provision of the Record of Authorization); and Section 3.1.4 (RDFI May Request Copy of Receiver's Authorization of Entry from ODFI).
[12] *See* Nacha Rules: Section 1.6 (Security Requirements); and Section 1.7 (Secure Transmission of ACH Information via Unsecured Electronic Networks).
[13] *See* Nacha Rules: Section 2.3.4 (Restrictions on Data Passing).
[14] *See* Nacha Rules: Section 2.2.3 (ODFI Risk Management).

should assess the impact that reliance on open banking data has on their respective Originators.

Nacha staff is continuing to work with industry representatives to assess the implications of the Final Rule and whether any enhancements to the Nacha Rules or applicable guidance are warranted to minimize any potential adverse impacts from the implementation of the Final Rule.

<p style="text-align:center">###</p>