



3138 10th Street North  
Arlington, VA 22201-2149  
703.522.4770 | 800.336.4644  
f: 703.524.1082  
nafcu@nafcu.org | nafcu.org

**National Association of Federally-Insured Credit Unions**

February 14, 2022

Comment Intake  
PRA Office  
Bureau of Consumer Financial Protection  
1700 G Street NW  
Washington, DC 20552

**RE: Agency Information Collection Activities: Comment Request (Regulation E)  
(Docket No. CFPB-2021-0021)**

Dear Sir or Madam:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU) I am writing in response to the request for comment (RFC) issued by the Consumer Financial Protection Bureau (CFPB or Bureau) regarding its Paperwork Reduction Act (PRA) review of information collected under Regulation E. NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 127 million consumers with personal and small business financial service products. The RFC calls attention to the Bureau's collection of information, such as required disclosures and records, that is used to evaluate financial institution compliance with Regulation E.

While NAFCU's comments primarily concern Regulation E's error resolution provisions, the Bureau must consider, as part of its PRA duties, "ways to minimize the burden of the collection of information on respondents." Unclear error resolution guidance targeting "token errors" and P2P payments contributes to added compliance burden for credit unions, and thus encompasses burdens related to information collection. Investigations of alleged unauthorized transfers may involve financial institutions providing a written explanation to the consumer asserting the payment error, and the burden of furnishing these explanations is within the scope of the CFPB's PRA review.<sup>1</sup>

To mitigate the compliance challenges associated with payment error investigations (and their associated information collection burdens), NAFCU asks that the Bureau clarify expectations around token error investigations, which may be difficult for a credit union to conduct without access to certain information, particularly when the underlying transfer involves a P2P service. The Bureau should also consider ways to achieve a more equitable balance of error resolution responsibilities that may be shared between financial institutions and P2P payment service providers.

---

<sup>1</sup> See 12 CFR § 1005.11(d)(1).

## General Comments

NAFCU recognizes that Regulation E's error resolution procedures help protect consumers from the risk of unauthorized electronic fund transfers initiated without individual consent. However, the Bureau's most recent guidance related to "token errors" has created uncertainty about what constitutes a reasonable investigation when these errors involve a third-party payment provider, such as a P2P provider.<sup>2</sup> Furthermore, the allocation of error resolution responsibilities to financial institutions for alleged P2P errors has created unfair compliance burdens for credit unions. As noted in a prior NAFCU letters, credit union members have responded to shortcomings in P2P customer service by turning to their primary financial institution for assistance with P2P-related errors, and this has shifted compliance burdens onto credit unions who may share error resolution responsibilities.<sup>3</sup>

Many credit union members are users of P2P payment services and business analysts estimate that by the end of 2023, \$1.1 trillion will transact over P2P platforms.<sup>4</sup> While these services are undoubtedly convenient and popular, their existence (along with an accompanying ecosystem of digital wallets) was not anticipated when the Electronic Fund Transfer Act (EFTA) was drafted and passed into law. Accordingly, the EFTA's decades old consumer protection framework for unauthorized transfers does not offer a hierarchical regime for allocating error resolution responsibilities when different private parties are involved at different stages of a payment transaction. As a result, credit unions that are only tangentially connected to P2P transactions because of a linked debit or credit card may share full responsibility for investigating alleged errors despite being in an inferior position to research the cause of the error and validate the consumer's claims.

While legislative amendments to the EFTA would be necessary to achieve a more efficient allocation of error resolution responsibilities between P2P providers and credit unions, the CFPB should consider opportunities for balancing investigatory responsibilities by taking into account the informational advantage of P2P providers when errors primarily arise through use of their platforms. The Bureau should also clarify its most recent guidance related to token errors and acknowledge that credit unions may face significant limitations when asked to investigate these errors in connection with P2P transactions.

### **The CFPB should consider more equitable mechanisms for allocating error resolution duties in the context of P2P payments.**

The CFPB's December 2021 updates to its Regulation E FAQs illustrate that in many cases, alleged errors occurring on P2P payment networks must be investigated by financial institutions,

---

<sup>2</sup> CFPB, Supervisory Highlights, Fall 2021, 6.

<sup>3</sup> NAFCU, Comment re: Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms; (Docket No. CFPB-2021-0017) (December 13, 2021), *available at* <https://www.nafcu.org/system/files/files/12.13.2021%20Letter%20to%20CFPB%20re%20Inquiry%20into%20Big%20Tech%20Payment%20Platforms.pdf>.

<sup>4</sup> See Insider Intelligence, "How the biggest mobile P2P payment players stack up," (April 19, 2021), *available at* <https://www.emarketer.com/content/breaking-down-mobile-p2p-payments-biggest-players>.

even when their only connection to the allegedly unauthorized transfer is the fact that a linked debit card or account was used (at some point) to pull funds into a P2P wallet. As the Bureau explains in FAQ - Coverage: Transactions #5,

“Generally, a “pass-through” payment transfers funds from the consumer’s account held by an external financial institution to another person’s account held by an external financial institution. A “pass-through” payment is initiated through a financial institution that does not hold a consumer’s account, for example, a non-bank P2P provider. [...] Regulation E applies to any EFT that authorizes a financial institution to debit or credit a consumer’s account.”<sup>5</sup>

The CFPB’s FAQs do not address certain factors that may complicate analysis of whether a payment is truly a “pass-through” payment. For example, the P2P-related FAQs which involve pass-through scenarios are premised only on the fact that funds are drawn into the P2P wallet from a debit card or account at a financial institution. The ability to draw a clear link to “pass-through” funds makes it relatively easy to determine whether a financial institution bears at least shared responsibility to investigate unauthorized EFTs that are P2P-related.<sup>6</sup> However, it remains unclear whether a financial institution bears similar responsibility if some of the funds involved in the unauthorized EFT are non-pass-through funds (i.e., not drawn contemporaneously from a consumer’s debit card or financial institution account) and originally acquired through the P2P network itself (e.g., received from other P2P users).

The Bureau should clarify that in instances where the value of an allegedly erroneous P2P transfer does not match a contemporaneous debit to a consumer’s linked account at another financial institution, the P2P provider bears primary responsibility (in the absence of an agreement with the financial institution) for investigating alleged payment errors. In these situations, where it is difficult for a financial institution to reasonably ascertain what mix of funds were used in the unauthorized P2P transaction, the P2P provider will be in a superior position to investigate and resolve the error. Consumers would benefit from such a clarification to the extent that P2P providers would be able to resolve disputes more accurately and with greater efficiency given that they possess all of the relevant information for analyzing transactions on their own platform.

**The Bureau must clarify expectations for investigating token errors before penalizing financial institutions for inadequate error resolution procedures.**

---

<sup>5</sup> CFPB, Electronic Fund Transfers FAQs (updated December 13, 2021), available at <https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>.

<sup>6</sup> *See id.* As the Bureau notes in FAQ - Coverage: Financial Institutions EFTs #4, where “an EFT is initiated through a non-bank P2P payment provider using a consumer’s debit card information, the P2P provider and the account-holding financial institution are parties to an agreement to honor each other’s debit cards – the debit card network rules – and the service provider provision in 12 CFR 1005.14, discussed in [Electronic Fund Transfers Coverage: Financial Institutions Question 1](#), does not apply [...] [a]ccordingly the account-holding financial institution has full error resolution responsibilities.”

The CFPB’s Fall 2021 Supervisory Highlights describes a type of Regulation E error that occurs when a consumer enters correct information (i.e., name, routing number, address, etc.) but “due to inaccurate or outdated information in the digital payment network directory,” the funds do not go to the intended recipient. The CFPB calls this a “token error.”

In the Supervisory Highlights report, the CFPB observed that institutions violated Regulation E by failing to determine that token errors constituted “incorrect” EFTs under Regulation E and by failing to conduct reasonable error investigations when consumers provided notice that they had sent funds via a P2P network, but that the intended recipients had not received the funds. Of note, the CFPB found investigations to be inadequate in this context when the financial institution reviewed only whether the transaction was processed in accordance with the sender’s payment instructions. The CFPB now takes the position that a reasonable investigation should consider whether the transfer may have gone to an unintended recipient due to a token error.

The Bureau’s brief description of a token error, in conjunction with its latest Regulation E FAQs, has created uncertainty about what constitutes a reasonable investigation of an error that involves a third-party P2P network.

The Supervisory Highlights do not provide any of the critical contextual detail that would help credit unions understand the standard of reasonableness the Bureau has chosen to advance for token errors. For example, it is unknown whether the financial institutions that failed to conduct reasonable investigations were operators of P2P payment networks because use of the term financial institution could refer to multiple entities with shared error resolution responsibility. Additionally, there is no description of the underlying payment flow which is critical for determining the applicability of Regulation E. For example, it remains unclear whether the token errors were “pass-through” transactions or if they involved stored funds that were originally acquired intra-network (e.g., from other P2P users).

Separately, the CFPB cites the failure of financial institutions to consult “relevant information” that could be reasonably acquired during an investigation to resolve an alleged token error but fails to specify the type of forensic data that a financial institution should consider or request. Some have inferred from the Bureau’s criticism that even when a financial institution does not have information that is responsive to token error claims, they will be penalized for failing to acquire it despite there being no industry-standard mechanism for requesting detailed network and transaction information from P2P providers. For example, chargeback requests through credit card companies stemming from P2P platforms do not include token information and there is no way to request that within the chargeback system.

NAFCU members have reported that third parties with whom their credit union has no contractual relationship are rarely responsive to requests to provide information related to Regulation E error investigations. Accordingly, it would be unreasonable for the Bureau to fault credit unions for not adequately investigating alleged P2P token errors when the availability of relevant forensic information resides almost exclusively with P2P providers. Further, under Regulation E, if a credit

union is unable to prove there was not an error, the member's claim must be honored.<sup>7</sup> Absent a contractual agreement with a P2P payment provider, there is minimal opportunity for a credit union to investigate token errors to determine whether a claim of unreceived funds is a legitimate token error or a fraudulent scheme. Fraudsters have already begun to trick consumers into sending multiple P2P transactions by stating the funds were not received. NAFCU members have also expressed concern that fraudsters will latch on to a new opportunity to defraud credit unions with a deluge of claims that must be honored.

To address uncertainty around token error investigations and provide a more equitable framework for institutions that do not have access to diagnostic information concerning the directory infrastructure of P2P services, the Bureau should specify that for P2P transfers, P2P providers should be primarily responsible for investigating token errors. Even if the transaction is a pass-through transaction, such that it would give rise to shared error resolution responsibilities with another financial institution (i.e., a debit card issuer), the P2P provider will still be in a superior position to investigate an alleged token error. Most, if not all, P2P services require users to enter recipient information through their own dedicated applications. Consequently, P2P providers will control the data and logic governing use of tokens and have greater investigative ability compared to financial institutions that are linked to P2P transactions only in a pass-through capacity.

## **Conclusion**

NAFCU supports clear and fair rules governing error resolution procedures for financial institutions. By clarifying expectations for token error investigations and considering a more equitable framework for allocating Regulation E responsibilities when transfers involve P2P services, the Bureau will improve consumer outcomes by supporting a more efficient error resolution process.

As NAFCU has noted in prior letters, credit union members will often prefer contacting their credit union when they have issues with P2P transfers since they believe the credit union is more responsive than the P2P operator. Credit union investments in high touch service models have incentivized this behavior but left credit unions shouldering a disproportionate compliance burden. Fully remedying this imbalance may necessitate Congressional action, but an adjustment of regulatory expectations for P2P-related investigations can mitigate some of the costs born by credit unions when members assert that a P2P transfer was unauthorized or executed incorrectly. Furthermore, providing greater certainty and fairness in the error resolution process will save credit unions and their member-owners money and time that could be used for service and product enhancements.

NAFCU appreciates the opportunity to provide comments on this notice. If we can answer any questions or provide you with additional information, please do not hesitate to contact me at 703-842-2266 or [amorris@nafcu.org](mailto:amorris@nafcu.org).

---

<sup>7</sup> See 15 U.S.C § 1693g(b).

Consumer Financial Protection Bureau  
February 14, 2022  
Page 6 of 6

Sincerely,

A handwritten signature in black ink that reads "Andrew Morris". The signature is written in a cursive style with a long, sweeping underline.

Andrew Morris  
Senior Counsel for Research and Policy