Independent Banker

May 2024

Portfolio

[tag] Checks & Balances

[hed] New Nacha rules strengthen security of the ACH system

[dek] Credit-push fraud in the ACH system has spurred the introduction of new rules from Nacha. With ICBA’s support, these new rules have changed how receiving institutions can address such fraud.

[byline] By Kari Mitchum

[body]

Recently, the banking industry has taken further initiative to tackle a concerning problem: Credit-push fraud. Also called authorized push payment (APP) fraud, credit-push fraud is when a consumer authorizes a payment but may have been fraudulently induced to do so.

In March 2024, Nacha—the organization that governs the ACH system—promulgated new rules that address some key factors behind credit-push fraud and will help community banks combat it.

ICBA supports these rules, as they update the existing procedures for combating credit-push fraud and clarify the roles of both the sending institution (ODFI) and the receiving institution (RDFI). The rules also outline the responsibilities of the third parties and originators in the ACH system: the payroll providers, billers and service providers—all the nonbank supporters that work together so consumers can receive direct deposit paychecks and make online bill payments.

[subhead] The extent of the problem

Here’s the issue: Even though this is called “fraud,” credit-push fraud payments are fully authorized by the consumer and not made under duress. The money gets “pushed” from a victim’s bank account to the account of a fraudster, and the ACH system, which moves more money than any other banking system, is a key target. The technology behind the ACH system is secure, meaning this fraud requires human interference, usually in the form of a scam.

One of the most common credit-push frauds is business email compromise (BEC). This occurs when a scammer uses email to trick someone into sending them money or doing something equally damaging, such as revealing personal or company account information.

To give you a better picture, the FBI received 21,489 complaints of BEC in 2023, according to the agency’s Internet Crime Report. These complaints entailed an estimated $2.9 billion in losses. The only type of fraud resulting in greater losses in 2023 was investment fraud.

[subhed] New rules extend time to examine

Nacha’s new rules require fraud monitoring at all levels. So, how does that affect your community bank? Well, RDFIs must now track incoming payments to detect fraud in an account. They could do this, for example, by questioning if a consumer account is receiving a business transaction. In essence, the rules establish a base level of ACH payment monitoring on all parties, except consumers.

With these new rules, the ODFI can request the return of the money for any reason if fraud is detected. The RDFI is now also permitted to take more time to examine the payment before releasing it. This will take some of the time pressure off community banks investigating suspicious ACH requests, which will subsequently help them block unauthorized transactions from hitting customers’ accounts.

While the new rules do not permit the receiving financial institution to hold money longer than the Federal Reserve Regulation CC allows, they do extend the time over the previous Nacha rules regarding this issue.

The RDFI, thanks to the new rules, can even return suspicious transactions without waiting for a request or a customer claim. After all, it’s hard to claw money back once a fraudulent transaction has been fully processed by both the originating and receiving financial institutions.

Under the new rules, consumers are empowered to report a fraudulent transaction before it posts via an update to the Written Statement of Unauthorized Debit (WSUD). This sensible change allows the fraud prevention process to kick off even while a suspicious transaction is pending. Previously, the transaction could not be reported until it posted.

Finally, the rules help improve transaction monitoring by applying a standard transaction description for ACH credits used for payroll payments. This is especially important for products such as early payroll access. Now, community banks will be able to clearly identify which payments are designated for payroll.

[subhed] ICBA’s advocacy work

ICBA has supported Nacha’s initiative to improve credit-push fraud prevention since the organization released its “Risk Management Framework for the Era of Credit-Push Fraud” strategy in 2022. This strategy expanded Nacha’s existing procedures for the detection and prevention of fraud to include credit-push payments.

Additionally, ICBA encouraged members to respond to a Nacha survey about the proposal, and members who did so expressed support for the proposed new rules and their potential impact on maintaining the safety and security of the ACH network.

To better accommodate the community bank industry, ICBA advocated for a phased rollout of the new rules that gives more time for them to comply. Nacha agreed, and a phased rollout for banks with an ACH volume of less than $10 million is reflected in the revised rules.

[subhed] Banks helping banks

These new rules are a great example of the banking industry working together to protect itself and consumers. The ACH system—the backbone of online banking—is not a government-run operation. By taking the initiative to improve the security of the system through sensible revisions to the Nacha rules, community banks are demonstrating they are united in the battle to fight fraud and keep the system secure, without government intervention.

**Kari Mitchum** is ICBA vice president, payments policy.

[end]

[pull quotes]

ICBA has supported Nacha’s initiative to improve credit-push fraud prevention since the organization released its “Risk Management Framework for the Era of Credit-Push Fraud” strategy in 2022.