The BSA Examiner©

A Quarterly Publication from Wayne Barnett Software
Volume 99, 4th Quarter 2025

The BSA Examiner is a quarterly newsletter published by Wayne Barnett Software. If you have a question to ask or a story to tell (we promise anonymity), please call us at 469-464-1902.

Case #1—FinCEN Alternative Collection Method to Obtain TIN

A long-time customer of a Midwestern community bank walked into a branch after her husband passed away unexpectedly. She needed to open an account in her own name so she could receive survivor benefits and begin managing household finances on her own.

She was shaken, overwhelmed, and missing paperwork — including her Social Security card. Under older interpretations of CIP, the conversation could have ended quickly: "We're sorry: please come back when you have your documents."

Instead, the banker did something different. Because the bank already had a long-standing relationship with the customer, the banker was able to:

- Access existing verified customer records,
- Confirm identity through internal systems,
- Use trusted third-party verification tools, and
- Walk the customer through reviewing and confirming pre-filled information.

The account was opened the same day. No shortcuts were taken. No rules were broken. But the process was human.

Later, the customer wrote a handwritten note thanking the bank — not for speed or convenience, but because "you treated me like a person when I needed it most."

In 2025, FinCEN issued an order granting an exemption for all accounts at all banks subject to the jurisdiction of the Board of Governors of the Federal Reserve System from a Customer Identification Program (CIP) Rule requirement implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l), related to a bank obtaining Taxpayer Identification Number (TIN) information from the customer. The exemption in this ORDER permits a bank to use an alternative collection method to obtain TIN information from a third-party rather than from the customer, provided that the bank otherwise complies with the CIP Rule, which requires written procedures that: (1) enable the bank to obtain TIN information prior to opening an account; (2) are based on the bank's assessment of the relevant risks; and (3) are risk-based for the purpose of verifying the identity of each customer to the extent reasonable and practicable, enabling the bank to form a reasonable belief that it knows the true identity of each customer.

The FDIC also issued FIL-39-2025 FDIC Supervisory Approach Regarding the Use of Pre-Populated Information for Purposes of Customer Identification Program Requirements. CIP requires an institution to collect certain information "from a customer" opening an account; however, the FDIC will now allow that information to be pre-filled/populated from other sources, such as current or prior accounts, affiliates, vendors, etc. that is then reviewed by and submitted by the customer. This will most likely involve digital/on-line account opening forms where fields are automatically filled in based on prior relationship or third-party data. The guidance is explicitly applicable to **FDIC-supervised institutions**.

The FIL states that when examining an FDIC-supervised institution that collects identifying information from a customer where some or all of the information was pre-populated, FDIC examiners will consider the pre-filled information as from the customer provided that
(1) The customer must have the opportunity and ability to review, correct, update, and confirm the accuracy of the information, and
(2) The institution's account-opening process (when using pre-populated information) must allow the institution to form a reasonable belief as to the identity of the customer — and must be based on a risk assessment of relevant risks (including risk of fraudulent account opening or takeover).
Click the link below for additional information.

https://www.fdic.gov/news/financial-institution-letters

Stories like this are why recent regulatory guidance around Customer Identification Programs matters. The updates issued by FinCEN and the FDIC in 2025 do not weaken identity requirements — but they do recognize that banks can meet those requirements in ways that reflect modern banking relationships, technology, and real customer needs.

Case #2—A Cautionary Bank Tale

At Smarter Faster Payments Remote Connect 2025, a payments executive, William Mills (VP of Deposit and ACH Operations at Premier Banks), shared a true story that illustrates why the new NACHA rules matter:

A branch manager called Mills about a suspicious ACH transaction. It turned out to be an ACH credit of $40,000 going to a personal account with only small debit card activity like Venmo/PayPal transactions.

The account showed "classic kiting indicators" — tiny deposits and nearly identical tiny withdrawals repeated many times — a red flag for fraud. This kind of pattern suggests fraud, such as money moving through mule accounts or unauthorized credits — exactly the types of problems the new rule changes are meant to address.

What the New NACHA Rules Are (and Why They Were Created)

These rule updates aren't random—they respond to shifts in fraud trends, particularly credit-push fraud: *The Fraud Trend That Triggered Change*

Instead of traditional debit fraud (money pulled from an account), criminals increasingly use credit-push fraud:

- They trick someone into authorizing a payment (e.g., via business email compromise or vendor
- Once the credit goes out, funds move quickly and are hard to recover.

This surge in sophisticated scams (BEC, payroll impersonation, vendor scams, mule accounts) convinced NACHA members that existing protections were not enough — hence new operating rules focused on fraud detection and prevention.

Key Rule Updates

Here are the major changes now rolling out (with dates and purpose):

1. *Strengthened Fraud Monitoring (March & June 2026)*

Originators, ODFIs, Third-Party Service Providers/Senders must build risk-based fraud monitoring processes to identify ACH entries that are:

- Unauthorized, or
- Initiated under false pretenses (e.g., social engineering fraud like BEC).

Phase 1 begins March 20, 2026 for high-volume parties; Phase 2 extends to all by June 22, 2026.

Why this matters: For the first time, fraud detection isn't just a best practice — it's a formal rule obligation across the ACH ecosystem.

2. *RDFI Credit Monitoring (2026)*
Receiving banks (RDFIs) must also implement processes to watch incoming ACH credits for potential fraud. This is new — RDFIs historically just posted credits without proactive monitoring.

3. *Standardized Company Entry Descriptions (March 20, 2026)*
Transactions like payroll and e-commerce must use specific descriptions ("PAYROLL" or "PURCHASE"), which helps monitoring systems identify transaction types more accurately.

4. *Faster Funds Availability (Sept 18, 2026)*
Standard ACH credits must now be available by 9:00 a.m. local time on settlement date, regardless of when they were received the day before — eliminating the old 5:00 p.m. cutoff.

5. *International ACH Transactions (IAT) Clarifications*
Updates clarify what counts as an IAT and require better contact registration — important for cross-border payments.

Why "Stories" Like This Matter

The bank branch story above isn't just an odd case — it illustrates a widespread problem NACHA is trying to fix:

- Fraudsters exploit gaps in monitoring
- Organizations often don't check unusual patterns
- Funds often move before fraud is detected

NACHA's updated rules aim to close those gaps by making fraud prevention proactive, documented, and risk-based — not just best practice.

Barnett Software's Suspicious Activity Monitor (SAM) portion of the software assists banks in continuously analyzing incoming and outgoing ACH activity against historical behavior. It uses behavior modeling to establish what "normal" looks like and then flags transactions that deviate from that pattern — exactly what a risk-based monitoring process in the NACHA rules calls for. But that's not all we do! Check out our website to learn more www.barnettsoftware.com

If you like the commonsense stories and guidance we tell in our newsletters, you'll love our easy-to-use software. We are Wayne Barnett Software. We're not a big company, but our products compare nicely with Verafin, Abrigo and the others. You can contact us at rrigdon@barnettsoftware.com or 469-464-1902. Thanks for reading our newsletter.