

ADVOCACY BRIEFING

The Wire Transfer Verification Act

Closing a 1989 banking loophole that costs Americans billions in fraud each year.

\$2.9B+

Estimated annual U.S. losses to business email compromise fraud

1989

Year the current UCC § 4A-207 verification rule was written

0

Statutory duty banks owe today to match a name to an account number

Executive Summary

Most Americans believe that when they wire money, their bank confirms it is going to the right person. They are wrong. Under Section 4A-207 of the Uniform Commercial Code — adopted in every state — a receiving bank is permitted to rely solely on the account number listed on a payment order, and is told it *need not* verify whether the name on the order matches the name on the account. The rule was written in 1989 for a paper-based payments system. It has become a structural enabler of modern wire fraud.

The **Wire Transfer Verification Act** closes this loophole. It requires receiving banks to confirm — using the same automated tools already standard in the United Kingdom and the European Union — that the name and account number on a payment order refer to the same person before the transfer is processed. Banks that skip the check and pay a fraudster bear the loss. Banks that perform the check are protected.

THE BOTTOM LINE

This bill requires what every American already assumes their bank is doing: looking at both the name and the account number before sending the money.

The Problem

How the current law works

UCC § 4A-207(b)(1) tells the receiving bank that, even when the payment order names one person and lists an account number belonging to a different person, the bank "may rely on the number as the proper identification of the beneficiary" and "need not determine whether the name and number refer to the same person." A bank is liable only if it had *actual knowledge* of the mismatch — a near-impossible standard for a victim to prove.

How fraudsters exploit it

The exploit is called **business email compromise**, and it works the same way every time. A criminal impersonates a vendor, executive, or attorney by email and tells the victim that "banking details have changed." The victim sends a wire. The wire instruction lists the legitimate recipient's name but a fraudster-controlled account number. The bank routes the funds to the fraudster, who withdraws within hours. The victim has no recourse against the bank — because the bank followed the law exactly as written.

A recent case in point

In *Studco Building Systems v. 1st Advantage Federal Credit Union* (4th Cir. 2025), a construction company lost more than half a million dollars to a fraudulent ACH transfer. The credit union deposited the funds into an account whose holder's name did not match the name on the payment order. The trial court held the credit union liable. The Fourth

Circuit reversed, ruling that under § 4A-207 the credit union owed nothing — because it had no actual knowledge of the mismatch and was under no duty to look.

WHY THE 1989 JUSTIFICATION NO LONGER HOLDS

The drafters of § 4A-207 worried that requiring name-and-number matching would "impede the efficient transfer of funds" in a world of manual processing. Today, automated matching is fast, cheap, and routine. The United Kingdom has required "Confirmation of Payee" since 2020; the European Union's Instant Payments Regulation requires it across the bloc as of 2025. The U.S. is now an outlier among developed economies.

The Solution

The Wire Transfer Verification Act flips the default. Where current law tells banks they may ignore a name-number mismatch, the bill requires them to catch it. The core changes are summarized below.

CURRENT LAW	PROPOSED CHANGE
Bank need not check that the name matches the account number.	Bank must verify, before processing, that the name and account number identify the same person.
Bank may rely on the account number alone, even when both fields are provided.	If the name and number do not match, the bank must halt the transfer, notify the originator, and seek corrected instructions.
Bank is liable only if it had actual knowledge of the mismatch — almost never provable.	Bank is liable to the originator if it processes a transfer it knew or should have known contained a mismatch.
Banks may contractually disclaim verification duties in customer account agreements.	Verification duty cannot be waived by contract with non-bank customers (small businesses, individuals).
Originator bears the loss in nearly all fraud scenarios.	Originator still bears loss when its <i>own</i> instructions are matching but wrong; bank bears loss when verification was skipped.

What the bill does *not* do

The bill does not impose strict liability. It does not require banks to investigate the underlying business relationship between an originator and a beneficiary. It does not change the originator's responsibility to provide accurate information. It does not weaken any consumer protections under the Electronic Fund Transfer Act. And it includes a documented-outage safe harbor for the rare case when verification systems are unavailable.

Key Provisions of the Bill

Section 4. Verification Requirement. Requires the beneficiary's bank to verify, before processing any payment order that includes both a name and an account number, that the two refer to the same person.

Section 4(b). Action on Mismatch. Requires the bank to decline the transfer, notify the originator, and return funds if corrected instructions are not received.

Section 4(c). Outage Safe Harbor. Permits transfers during documented verification-system outages only with the originator's recorded consent. The originator then bears the risk.

Section 5. Liability. Holds banks liable to the originator for the amount of the transfer, plus interest and reasonable costs, when verification is skipped or negligently performed. The duty cannot be disclaimed in non-bank customer agreements.

Section 6. Preemption. Preempts state UCC § 4A-207 to the extent it conflicts with the federal standard, while preserving stronger state-law protections and all federal consumer protections.

Section 7. Rulemaking. Directs the CFPB, in consultation with the Federal Reserve and OCC, to issue implementing regulations within 18 months.

Section 8. Effective Date. Takes effect 24 months after enactment, allowing financial institutions adequate time to deploy verification systems.

Who Benefits

Small businesses and nonprofits. The hardest-hit victims of business email compromise. A single fraudulent wire can wipe out a year's payroll. Most do not have the resources to litigate against a bank or chase a fraudster overseas.

Individual consumers. Real estate closing fraud — where buyers wire down payments to fraudsters posing as title companies — is one of the fastest-growing categories of consumer fraud. The bill prevents the wire from clearing in the first place.

Honest banks. Many financial institutions already perform name-and-number matching voluntarily. A uniform standard levels the playing field and prevents a race to the bottom in which lower-diligence banks become preferred fraudster destinations.

Law enforcement. Stopping fraudulent transfers before they clear is dramatically more effective than trying to recover funds after they have been laundered through cash-out networks.

Anticipated Objections and Responses

Objection: *"This will slow down payments."*

Response: Confirmation-of-payee systems in the UK and EU operate in milliseconds. They are embedded in real-time payment networks specifically designed for speed. The cost of a brief verification check is trivial compared to the cost of fraudulent loss.

Objection: *"This will impose unfair burdens on community banks."*

Response: The 24-month effective date and CFPB rulemaking process are designed to give smaller institutions time to adopt vendor-provided verification services. Many core banking platforms now offer name-matching as a built-in feature.

Objection: *"The originator should bear responsibility for accurate instructions."*

Response: The bill preserves originator responsibility for instructions that are matching but wrong. It only assigns liability when the bank fails to catch a mismatch its own systems can identify. This is the same allocation that applies in every other major developed economy.

Objection: *"This duplicates existing fraud-prevention rules."*

Response: It does not. No federal or state statute currently requires name-and-number verification. Existing rules — including BSA/AML and Reg E — address different problems. This bill addresses the specific gap left by UCC § 4A-207.

WHAT YOU CAN DO

Members of Congress: Co-sponsor the Wire Transfer Verification Act when introduced. **Staff:** Contact the lead sponsor's office for the section-by-section, draft floor statement, and Legislative Counsel-ready bill text. **Outside organizations:** Sign on to the coalition letter; submit statements of support through Government Affairs.