

WIRE & ACH TRANSFER FRAUD.



Almost every successful wire or ACH fraud hinges on one moment: a payment instruction change that looks legitimate enough to act on without independent verification. **Once a transfer executes, it's effectively irrevocable — the control has to work before the money moves, not after.**

- OUT-OF-BAND VERIFICATION
- DUAL CONTROL
- VENDOR CHANGE FRAUD
- IRREVOCABLE TRANSFERS

01 THE MECHANISM

The Instruction Change Is the Attack

Almost every successful wire or ACH fraud hinges on a single moment: a payment instruction — a new account, a changed routing number — that **looks legitimate enough to act on without independent verification.**

Callback Verification Breaks the Chain

Calling a previously known, independently verified phone number — never one supplied in the suspicious instruction itself — is **the single control that stops most BEC-driven wire fraud** before it happens.

Execution Is Effectively Irrevocable

Unlike a check, a completed wire settles fast and is designed to be final. **By the time fraud is discovered, the funds have often already been withdrawn** or moved again.

02 THE FLOW

The Verified Payment Change CONTAINED

- 1 A vendor emails a routing number change; accounts payable **independently calls the vendor's previously verified phone number**, not the number in the email, to confirm.
- 2 The change is entered only after a second approver signs off, and the **first payment to the new account is held for manual review.**
- 3 Even if the original email was fraudulent, the callback **catches the impersonation before a single dollar moves.**

The Unverified Payment Change EXPOSED

- 1 A convincing email, apparently from a known vendor or executive, requests an urgent routing change, with a **phone number conveniently included** "for questions."
- 2 The employee calls the number in the email to confirm — **reaching the attacker**, who confirms their own fraudulent instruction.
- 3 The wire executes and settles within hours; by the time the real vendor asks where their payment is, **funds have already moved through multiple accounts.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Out-of-Band Verification	Confirming any payment instruction change via a previously known contact channel, never one supplied in the instruction itself.
Dual Control & Segregation of Duties	Separating who can initiate a transfer from who can approve it, so no single compromised or coerced individual can move funds alone.
Positive Pay & Debit Blocks	Bank-side controls that flag or reject transactions that don't match a pre-authorized list of payees, amounts, or originators.
Vendor Master File Change Controls	Mandatory verification and dual approval before a changed bank account can be used for any AP payment.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Verifying Changes Using Contact Info in the Instruction Itself	No	Calling a number supplied by the same email requesting the change just confirms the fraud with the attacker, not the real vendor.
Same Employee Initiates and Approves Transfers	No	A single compromised or coerced account can move funds with no independent check to catch it.
Relying on Post-Fraud Recovery Through Law Enforcement	No	Recovery windows are extremely short, and success is far from guaranteed once funds clear and move again.
Fraud Detection Without Payment-Layer Controls	No	Detecting an anomaly after a transfer has already settled is too late to stop irrevocable funds movement.
Out-of-Band Verification + Dual Control + Positive Pay + Vendor Change Controls	Yes	Catches a fraudulent instruction at the point where it can still be stopped, before funds move.

WIRE & ACH TRANSFER FRAUD.

VERIFY · APPROVE · MONITOR

05 PROGRAM OPERATIONS

The **callback number** has to come from a source independent of the instruction being verified. A phone number included in the same suspicious email is worthless as verification.

Business accounts have far weaker legal protection than consumer accounts. Regulation E's unauthorized-transfer protections don't extend to commercial accounts the way they do to individuals.

Under UCC Article 4A, a bank that offers and follows a commercially reasonable security procedure generally isn't liable for a fraudulent wire — declining it shifts real financial risk onto the business.

Speed cuts both ways. Same-day ACH and real-time wire settlement are good for business, but they also shrink the window to catch and reverse fraud before funds are gone.

06 CONTROL MAPPING

UCC ARTICLE 4A

The commercial code governing wire transfers in the US, establishing the "commercially reasonable security procedure" standard that determines liability.

REGULATION E

Electronic Fund Transfer Act protections for unauthorized transfers, applying to consumer accounts but explicitly not to business/commercial accounts.

NACHA OPERATING RULES

The ACH network's rules requiring originating institutions to implement fraud monitoring and data-security practices.

FBI IC3 RECOVERY ASSET TEAM

The mechanism for reporting fraudulent transfers quickly enough to attempt an international fund freeze, though the window is narrow.

07 WHAT THIS DOES NOT SOLVE

Recovery After Funds Clear

Once a fraudulent transfer settles and moves again, **recovery becomes unlikely** regardless of how quickly it's reported.

Insider-Initiated Fraud

Dual control raises the bar, but a **coordinated scheme involving both the initiator and approver** isn't fully solved by segregation of duties alone.

The Initial Compromise

These controls stop a fraudulent instruction from executing; they **don't prevent the phishing or BEC** that produced the instruction in the first place.

A Patient, Well-Researched Attacker

An attacker who studies real vendor relationships and timing can still **produce an instruction convincing enough to test every control**.

08 MYTHS VS. REALITY

MYTH "If fraud is reported quickly, the bank can just reverse the wire."	REALITY Wire transfers are designed to be final once executed; recovery depends on freezing funds before they're withdrawn again, and the window is very short.
MYTH "Calling the number in the email to confirm is good enough verification."	REALITY If the email is fraudulent, so is any contact information it provides — verification requires an independently sourced number.
MYTH "Our bank is liable if we get defrauded on a wire transfer."	REALITY Under UCC Article 4A, a bank that offered and followed a commercially reasonable security procedure generally isn't liable, even for a fraudulent wire.
MYTH "Business accounts have the same fraud protections as personal accounts."	REALITY Regulation E's unauthorized-transfer protections apply to consumers, not business accounts, leaving companies with substantially less legal recourse.
MYTH "ACH fraud is less serious than wire fraud because it's reversible."	REALITY Same-day ACH settles quickly, and business-to-business ACH has far weaker reversal protections than consumer transactions.

09 SPEAK THE PROGRAM — KEY TERMS

OUT-OF-BAND VERIFICATION Confirming a payment instruction through a contact channel independent of the instruction itself, such as a previously known phone number.	DUAL CONTROL Requiring two separate individuals to initiate and approve a payment, so no single compromised account can complete a fraudulent transfer.	UCC ARTICLE 4A The US commercial code governing wire transfers, establishing the liability standard based on security procedure adequacy.
REGULATION E The EFT Act's implementing regulation, providing unauthorized-transfer protections to consumer accounts but not business accounts.	POSITIVE PAY A bank service that flags or rejects transactions not matching a pre-authorized list of payees, amounts, or originators.	ACH DEBIT BLOCK A control instructing a bank to reject all ACH debits by default, or only permit them from a pre-authorized list of originators.