KEYSTONE ADVANCED SOLUTIONS · INTERNATIONAL FRAUD AWARENESS WEEK

The Payment Verification Checklist. *Callback before cash.*

Business email compromise cost U.S. victims $3.05 billion in 2025, and 86% of it left by wire or ACH. These are the rules our own team follows. Tape it next to the screen of anyone who touches payments.

BEFORE MONEY MOVES

- [ ] Any new payee or changed bank detail is confirmed by phone, on a number you had before the request arrived.
- [ ] Never use the phone number, link, or reply address in the message asking for the change.
- [ ] Write down who called whom, the number, the date, and what was confirmed, before anything is entered.
- [ ] Urgent, confidential, or “don’t loop anyone in” means slower, not faster.

WHO CAN MOVE IT

- [ ] The person who sets up a payee is not the person who releases the payment.
- [ ] Release limits live in the bank’s system, not in anyone’s memory.
- [ ] Two approvals above your threshold.
- [ ] Payroll and direct deposit changes get the same callback, to the employee on a number on file.

LOGINS AND DEVICES

- [ ] Multi-factor authentication on email, banking, and payroll. Never turned off to save time.
- [ ] Bank logins from a saved bookmark, never a search result or sponsored ad.
- [ ] No one ever shares a one-time code. A caller who asks for one is the attacker.
- [ ] Check your mailbox for forwarding or auto-delete rules you didn’t create.

STOP AND CALL BACK IF YOU SEE

- New bank details, especially right before a payment run
- Urgency or secrecy
- A sender address one character off
- A real thread that suddenly asks for money
- Won’t talk by phone or video
- A request for W-2s or payroll data
- A familiar voice or face asking for a payment on a call

IF MONEY ALREADY MOVED: THE FIRST HOUR

1. Call your bank’s fraud line and ask for a recall, plus any hold harmless letter it needs.
2. File at ic3.gov right away, whatever the amount, with the full transaction details.
3. Change passwords, end sessions, and check for mailbox rules.
4. Keep every email with headers, screenshots, and transaction records.

No money moves on email, voice, or video alone.

In 2025 the FBI helped freeze $679 million across 3,900 cases. Speed is what gets money back.

Sources: FBI Internet Crime Complaint Center, 2025 Annual Report and PSA I-112525-PSA (Nov 2025); U.S. Secret Service, Business Email Compromise; ACFE, Occupational Fraud 2026: A Report to the Nations. This checklist is general guidance, not legal or security advice for your specific systems.