

MBIS | BANK WIRE FRAUD

Wire Fraud – Insurance Implications

Customer BEC • employee deception • written agreements • callbacks • PINs • evidence

1

Business Email Compromise (BEC) and funds transfer fraud made up 58% of Cyber claims.

31%

**BUSINESS EMAIL
COMPROMISE**

27%

**FUNDS TRANSFER
FRAUD**

58%

**COMBINED SHARE
OF CLAIMS**

+15%

**BEC frequency
year over year**

≈ \$27K

**average BEC
severity**

≈ \$141K

**average FTF
loss**

Coalition 2026 Cyber Claims Report; claims reported during 2025. Dataset is cross-industry—not bank-only.

2

Direct-to-bank instructions raise both severity and control scrutiny.

20%

of Funds Transfer Fraud claims involved fraudulent instructions sent directly to a bank

≈ \$218K

average loss in those direct-to-bank events

\$21.8M

stolen funds recovered

≈ \$202K

average recovery

32%

Funds Transfer Fraud events with at least a partial recovery

Control implication: authentication evidence matters before release; escalation speed matters immediately after.

MBIS

3

Different entry points. The same target: a valid-looking wire or ACH request.

BANK EMPLOYEE DECEPTION

The attacker directs the bank employee

- Executive, customer or vendor impersonation
- Urgency, secrecy or exception pressure
- May exploit help desk or enrollment workflows

CUSTOMER BEC

The attacker speaks as the customer trying to trick another employee of the customer to send funds

- Compromised mailbox or online-banking credentials
- Changed beneficiary or payment instructions
- May pass ordinary identity questions

The wire platform can work exactly as designed—and the transaction can still be fraudulent.

MBIS

4

Insurance requirements for banks involving not in person ACH/ wire requests (phone ,fax, or email)

1	Written Agreement	Agreement expressly authorizes phone, fax or email instructions
2	Authorized person	Agreement identifies each person permitted to request wires
3	Trusted callback	Agreement states the telephone number the bank must call
4	Predetermined PIN/passcode	Customer-selected PIN/passcode appears in the agreement
5	Actual execution	Bank uses that number, verifies that credential and documents the call

NO AGREEMENT = STOP

Years of accepting informal instructions do not replace a complete written agreement—or expand it to a new channel.

MBIS

5

Scenario 1: the bank makes a callback—but not the required one.

A hacked bank customers email sends new wire instructions. The bank employee calls the number included in the email—or another number that is not on the written wire agreement.

The employee speaks with someone.
The request sounds legitimate.
The predetermined PIN/passcode is not obtained or verified.

WHY THE CLAIM IS EXPOSED

- Wrong callback number
- Person not verified under agreement
- No predetermined PIN/passcode match
- Wire details not authenticated
- Verification ledger incomplete
- Policy procedure not proven

A callback is not enough unless it is the required callback.

MBIS

6

A callback is only strong when the fraudulent channel is excluded.

STRONG CALLBACK

- Call the person and number in the written agreement
- Obtain and verify the predetermined PIN/passcode
- Confirm beneficiary, amount and wire purpose
- Complete and sign/initial the verification ledger
- Record the call when the carrier requires it

CALLBACK THEATER

- Number supplied with the wire request
- Number stored elsewhere but absent from the agreement
- Inbound return call or voicemail approval alone
- Generic questions instead of the required PIN
- "Known customer" or urgency exception

Coverage may depend on using the agreement-listed number and completing every required verification step.

MBIS

7

PINs and passcodes are evidence—not magic.

For many policy provisions, the PIN/passcode must be...

IN THE AGREEMENT

Documented in the executed written agreement between the customer and bank.

PREDETERMINED

Selected by the customer before the wire request—not created during the callback.

VERIFIED BY THE BANK

Obtained and matched by the bank employee before the wire is released.

Insurance consequence

No documented PIN, a PIN created during the request, or an unverified PIN may defeat an otherwise plausible claim.

MBIS

8

The same fraud can produce a different coverage outcome.

POTENTIALLY COVERED CLAIM

Fraudster compromises the customer's phone system and obtains the PIN.

- Written wire agreement is on file
- Bank calls the person and number in the agreement
- Employee verifies the predetermined PIN
- Required procedure and evidence are completed

COMMON DENIAL FACTS

The bank cannot prove literal compliance with the policy procedure.

- No written agreement for the customer
- Callback made to the fraudster's supplied number
- PIN verification is missing or undocumented
- Required ledger, signature or recording is absent

Following the procedure may preserve coverage even when the fraudster defeats the customer's controls.

MBIS

9

Scenario 2: a hacked customer email introduces a "new CFO."

THE FRAUDULENT REQUEST

"I'm the new CFO. Please add me to the wire form and use this number for future callbacks."

- Message comes from the commercial customer's real email
- New person, authority and callback data arrive together
- Fraudster is trying to become an authorized verifier

THE REQUIRED RESPONSE

- Do not amend authority from email alone
- Call an existing authorized person at the number already on the agreement
- Verify the request with the existing predetermined PIN/passcode
- Require an executed agreement amendment and dual approval
- Do not let the proposed new CFO verify their own addition

A change to the wire agreement is itself a high-risk funds-transfer event.

MBIS

10

Six controls must work in practice—not only on paper.

1 Confirm a complete written agreement authorizes the method

Before accepting phone, fax or email instructions, locate the agreement and all required authorization details.

2 Call the authorized requester at the number in the agreement

Never rely on a number in the wire request, email signature, forwarded thread or recently changed contact record.

3 Require and verify the predetermined PIN or passcode

The requester must provide the agreed credential during the callback, and the bank must verify it.

4 Separate instruction changes from transaction approval

A new CFO, signer, phone number, email, device or credential requires its own controlled verification.

5 Escalate exceptions instead of improvising

Urgency, executive status, travel, unavailable approvers or customer frustration must trigger escalation.

6 Create a usable record

Document who called, the trusted number used, who answered, what was verified, when and who approved exceptions.

If the customer cannot satisfy the agreed procedure, delay or refuse the wire—do not improvise.

MBIS

11

Customer BEC creates two separate insurance questions.

BANK'S COVERAGE + LIABILITY

Does the bank have to reimburse—and will its insurance even cover the loss?

- Customers often look to the bank first, regardless of ultimate liability
- The bank still must satisfy its own written-agreement, callback and PIN conditions
- The customer's insurance does not cure the bank's failure to follow its policy procedure

COMMERCIAL CUSTOMER'S COVERAGE

Does the customer have insurance that will cover the stolen funds?

- Many forms impose callback, voice-verification, in-person or dual-control conditions
- Failure to follow the exact procedure may defeat coverage
- MBIS specialized Cyber Deception option removes the traditional callback requirement

Ask first: Who was deceived? Whose funds moved? Which party followed which policy procedure?

MBIS

07

12

Scenario 3: a compromised CEO (customer of the bank) email triggers a \$240,000 wire.

THE FRAUDULENT REQUEST

“Send the \$240,000 today. This invoice is past due and I don’t want any more fees.”

- Finance manager receives the message from a vendor or the CEO’s genuine—but compromised—mailbox
- Email supplies wire instructions
- No independent callback is made to the CEO from the customer’s finance manager
- Finance manager is on the authorized wire agreement already
- Finance manager calls wire instruction into the bank and all callbacks and PIN/passcode verifications are completed by the bank

WHY THE CUSTOMER MAY BE UNCOVERED

Trust replaced the verification required by the customer’s policy.

- Customer’s cyber form requires callback or voice verification
- Finance manager skipped the required verification step
- Customer’s claim may be denied for noncompliance
- Bank processed authenticated instructions and may not owe reimbursement

Without specialized coverage, the customer may absorb the entire \$240,000 loss.

MBIS

07

13

MBIS coverage can change the customer’s outcome.

WITHOUT SPECIALIZED COVERAGE

Customer follows the fraudulent email—but not the required callback.

- Fraudster compromises an executive’s email and sends new ACH/wire instructions
- Employee sends funds without an independent callback
- Customer’s policy requires callback or voice verification
- Claim may be denied because the condition was not completed

WITH MBIS ACH/WIRE FRAUD COVERAGE

The same loss may be eligible without a callback condition.

- Optional coverage eliminates the traditional callback requirement
- The customer still must satisfy the remaining policy terms
- If purchased before the loss, the ACH/wire fraud may be covered
- Bank liability and the bank’s FI Bond analysis remain separate

Same fraud. Different result: the customer’s policy wording determines whether the missing callback defeats coverage.

MBIS

07

14

MBIS | MIDWEST BANKERS INSURANCE SERVICES

Questions

Adam Dawson

Regional Sales Manager

952-261-8978

adamd@mbisllc.com

mbisllc.com

Insurance for banks—from people who know banks.