What to do in the Event of Fraud

The following is recommended Citi Commercial Bank advice on steps to take in the event of suspected or actual fraud involving bank payments.

Act Quickly

Review and urgently determine if fraud has occurred; every minute may count.

To report fraud, contact the following:

Credit Card Fraud – Contact the number on the back of your card. Other types of fraud including ACH, CitiBusiness® Online, checks and wires – Contact your Citibank representative.

Use the "F" Word

Be prepared to state "fraud" – not "potential fraud" or similar as banks may not act on "potential" issues – and confirm this in writing/email.

Alert Citi and/or Beneficiary Bank Immediately

Citi will initiate recall actions.

The shorter the time between a fraudulent transaction and detection, the greater the chance of recovery (ideally less than 48 hours, thereafter the prospect of recovery drops off dramatically).

Provide the Details

Beneficiary banks and others will need clear background information before they will act.

Some jurisdictions make the recovery of misappropriated funds more difficult than others, so you may require further actions to recover your assets. For example, there may be legal restrictions on freezing/returning funds locally, or providing information on the identity of the beneficiary or remaining balance without a court/police order. There may also be certain processes that you, as the sender, may need to follow.

Further Recommended Steps	Reason/Example
Engage internal fraud/security resources	Bring in subject matter experts
Report to local law enforcement as soon as possible – obtain a copy of the report or take a crime reference number	Beneficiary banks may expect/ request this
Independently review all recent transactions and logs for other suspect payments or unusual activity	Look for other potentially fraudulent activity that may have occurred
Independently secure your bank accounts to prevent further misuse	For example, disable system users, implement payment exception approval process, etc.
Alert any other banks you may hold accounts with	In case fraudsters attack other bank accounts
Send an internal alert to increase awareness and vigilance	In case of further contact/attempts, unless there is a concern of internal compromise
Retain and hold any potential evidence for investigation	Examples of evidence include email correspondence, audio logs, desktop PCs
Consider appointing legal counsel, forensic consultants or private investigators to represent/assist you if necessary	Some jurisdictions can be more difficult to navigate than others
With your legal advisers' direction, question employees carefully to seek verification of their activity and keep written records of responses.	Ensure your employee's recollection of events is accurate

1507623 01/17