WHAT TO DO IN THE EVENT OF FRAUD

The following are some of the steps that should be taken in the event of suspected or actual fraud involving bank payments

First Response

- **Act Quickly:** Do not delay in notifying your bank about any suspected fraud. The shorter the time between a fraudulent transaction and detection, the greater the chance of recovery (ideally 24-48 hours, thereafter the prospect of recovery drops off dramatically). Every minute counts.
- **Alert your banks and Use the 'F' Word:** Be prepared to state "fraud" and confirm this in writing/email (not "potential fraud" or similar, banks will not act on "potential" issues). Your bank will then initiate recall actions, if possible.
- **Provide the Details:** Provide full transaction details and as complete (as possible) background details on the fraud. Your banks and others will need clear background information before they will act. Some jurisdictions may require further action so ensure you are aware of local requirements.
- **Provide Indemnity:** Always be prepared to provide your bank with indemnity to facilitate bank-to-bank recovery.
- **File a Police Report:** File a police report in both the remittance and ultimate beneficiary jurisdictions. Obtain a copy of the report or take a crime reference number as this may be requested from beneficiary banks.
- **Secure your accounts:** Independently secure your bank accounts to prevent further misuse. For example, disable system users, implement payment exception approval processes etc. Alert all other banks that you hold accounts with.

Additional Incident Handling

Phase 1

- **Legal Counsel:** Consider appointing legal counsel to navigate recovery of funds if recommended by your bank or law enforcement.
- **Internal Resources:** Ensure your internal fraud/security resources are engaged as the subject matter experts. Implement a communications plan (both internal and external) so that key stakeholders are aware and vigilant.
- **Review transactions:** Independently review all recent transactions and logs for other suspicious payments/unusual activity across all bank accounts.
- **Investigate:** Initiate an internal investigation. Ensure that any potential evidence is retained and secured. Examples of evidence include email correspondence, audio logs, desktop PCS etc.
- **Forensic Analysis:** Complete a digital forensic analysis for malware and points of compromise.

  For email and/or invoice Fraud:

  - Query relevant employees on any recent urgent high-value payments or beneficiary account change requests.
  - Alert suppliers/vendors on possible fraudulent invoice/account payee change requests.
  - Review malicious domain name registrations, websites and/or email accounts used to perpetrate the attack. Report the abuse to the relevant Domain Registrar(s).

Phase 2

- **Review:** Conduct a full review of controls - Implement new measures as necessary.

Post Fraud/Attack

- **Develop a Cyber Response Playbook:** Draw up a response plan /playbook for handling fraud incidents. The plan should be documented and widely socialised with employees, clearly defining roles and responsibilities clearly including escalation points of contact, information that needs to be conveyed and how the response should be managed.
- **Develop Protocols:** As part of the Cyber Response playbook, consider creating robust structures and protocols for the internal escalation of fraud including, for e.g. templates for emails and pre-defined mailing lists.
- **Staff Training:** Provide regular and updated fraud awareness training to ensure all employees are aware of current fraud threats, methods being used by fraudsters as well as the points of escalation and the Cyber Response Plan.
- **Monitor:** Continue to monitor supplier/vendor relationships and regularly check to ensure contact and other information with payers and payees is up to date.

Visit www.citibank.com/treasuryandtradesolutions/fraudpreventionresources for more information

Treasury and Trade Solutions