Commercial Bank

Guidance on How to Combat Fraud

Warning Signs

Fraudsters and cyber criminals are becoming more sophisticated in their methods and constantly evolving their techniques. They employ social engineering tactics and deception to commit fraud. **Be vigilant:** recognizing the signs of fraud is the most effective way to combat it.

Do you know what to look out for?

- Company executive name-dropping to rush transactions
- Alarmist or overly complimentary language
- Abusive or aggressive requests to transact
- Changes in your bank or supplier's usual tone or demeanor

- Badly written requests, with poor grammar, syntax, or spelling
- Changes to the normal appearance of the communication
- Requests to deal with unfamiliar contact names or contact details
- Email address variations or unfamiliar domain names

- Customers' or suppliers' known contacts are unreachable
- Calls purporting to be from financial institutions or suppliers

Are you being asked to...

- Take unsolicited calls from unknown contacts
- Contact new or unusual numbers
- Share your credentials (password, tokens, or other sensitive information)
- Accept enclosed or unconfirmed contact details
- Click on unexpected or unknown links in an email

- Circumvent normal procedures and policies
- Deal with first-time or unknown payment beneficiaries

- Approve unknown or unfamiliar transactions
- Transfer funds by, or before, a public holiday
- Transfer multiple sums to a new, unverified beneficiary

Do's and Don'ts

Cross-departmental co-operation is required to develop robust fraud prevention processes, policies, and plans.

Do...

- Work with all departments across your organization in the development of fraud prevention procedures. Each department will have a role to play and every employee should be aware of what to do in the case of suspected fraud.
- Host regular Staff training sessions.
- Stay informed on latest trends and threats.
- Use anti-virus, anti-spyware, and anti-malware software that updates automatically.
- Install applications or software from reputable providers that you know you can trust.
- Turn on your browser's pop-up blocker to stop malware attacks.
- Log out and close your browser when you finish your banking session.
- Use the most current version of your preferred browser.
- Password-protect any devices that you use to access a banking website.
- Be suspicious of unsolicited phone calls from individuals you do not know.
- Hang up if you are in doubt about a call, then call or email your known Citi contact.

Don't...

- Have uncoordinated fraud prevention trainings and no sign fraud prevention process.
- Use a computer without anti-virus, anti-spyware, and anti-malware detection software for online banking.
- Install applications or software from unknown sources or companies you do not trust.
- Use technology without a native or third-party pop-up blocker to defend against malware.
- Leave your browser window open on devices after you have logged into a password-protected site.
- Use outdated versions of browsers.
- Access financial information on any device or technology that is not password-protected.
- Share your passwords with anyone (Citi will not ask you to share this information).
- Click on any email links from unknown or unexpected senders.
- Share desktop screens with any unauthorized person.

Risks and Controls

These tips — when applied alongside your own internal control processes — will help reduce the risk involved in changing beneficiary's payment details.

PERFORM checks to reduce fraud risk.
- Validate payment instructions for any new counterparty with a trusted supplier or contact.
- Confirm requests, or any changes, in writing and with a phone call to known contacts.

MANAGE high-risk transactions.
- Configure your systems to require dual approval for sensitive business activities.

REDUCE business-wide transaction risk.
- Segregate duties for sensitive business activities.

UNDERSTAND social engineering.
- Promote training on cyber threats/fraud awareness.

CHECK activity.
- Regularly review your transaction reports.

CREATE a robust Maker/Checker process.
- Design an internal maker/checker processes to verify and approve account changes and activity.
- Implement a process for adding or changing beneficiary information.

PREPARE for risks posed by Generative Artificial Intelligence (AI).
- Call back on a verified telephone number if you are suspicious of a communication.
- Reconcile your account(s) frequently and report any potential discrepancies to your bank as quickly as possible.

Know the Fraud Landscape

Fraudsters may...

- Operate across markets, sectors, and geographies.
- Work in more creative, sophisticated ways.
- Make attempts to redirect payments.
- Seek to change beneficiary bank details.
- Hope you will accept forged letterheads.
- Attempt to notify you of bank changes.
- Pose as new account managers/bank technicians.
- Hack senior email accounts to request a payment.

IF YOU ARE A VICTIM OF AN ATTACK, IMMEDIATELY CONTACT YOUR BANK, LAW ENFORCEMENT, AND ESCALATE APPROPRIATELY WITHIN YOUR ORGANIZATION.

2344153 02/25