





## Guidance on How to Combat Fraud

### Warning Signs




#### For email, letter and phone

How do you know the email, letter or call you received requesting information or instructing a transaction is not fraudulent? Fraudsters exploit human psychology and other social engineering tactics in an attempt to commit fraud. Be vigilant: recognizing signs of fraud is the most effective way to combat it.

#### Have you noticed?

- 
  - Alarmist or perhaps overly complimentary language
  - Abusive or aggressive requests to transact
  - Changes in a customer's usual tone or demeanour
  - Suggestions of losing money if you fail to act
  - Company executive name-dropping to rush transactions
- 
  - Badly written requests, with poor grammar, syntax or spelling
  - Changes to the normal letterhead or appearance of the email
  - Alternative contact names or details provided
  - Email address variations or domain name changes
- 
  - Customers/suppliers calling in before callbacks can be made
  - Changes in a customers'/suppliers' usual callback number
  - Customers'/suppliers' known contacts are unreachable
  - Customers'/suppliers' seem anxious to complete transactions
- 
  - Unfamiliar suppliers or altered transaction details
  - Additional system login steps or transaction pages
  - System instructions that "appear" mysteriously

#### Are they asking you to . . .


- 
  - Receive unsolicited calls from unknown contacts
  - Contact new or unusual numbers
  - Give a password in a place you do not recognize
  - Accept enclosed or unconfirmed contact details
  - Receive or act on unsolicited instructions
  - Click on unexpected or unnecessary links in an email
- 
  - Circumvent normal procedures
  - Deal with a first-time or unknown payment beneficiary
  - Provide payment confirmation by email
  - Carry out instructions quickly after a profile change
  - Make immediate or urgent payment changes
  - Transfer most - or all - of the account balance
- 
  - Approve an unknown or unfamiliar transaction
  - Transfer funds by or before a public holiday
  - Transfer funds to a known secrecy haven
  - Transfer multiple sums to a new beneficiary
  - Transfer funds to an alternative jurisdiction

### Do's and Don'ts


#### For devices (smartphones, tablets, laptops and pcs)

You may need to involve your IT department to effectively adopt these recommendations. This may require that you undergo a risk assessment in compliance with your IT department's controls and evaluations.

#### Do . . .

- 
  - ✓ 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.
  - ✓ Enable your browser pop-up blocker to avoid malicious software attacks.
  - ✓ Log out and close your browser when you finish your banking session.
  - ✓ Use 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 any 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 . . .


- 
  - ✗ 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 challenge response with anyone (Citi will not ask you to share this information).
  - ✗ Click on any email links from unknown or unexpected senders.
  - ✗ Share PC screens with any unauthorized person.

### Risks and Controls

#### For beneficiary change requests


Recognizing the problem is the key to applying best practice solutions. These tips – when applied alongside your own internal control processes – will mitigate the risk involved in changing beneficiary's payment details.

-  **The risks with fraudsters are that they . . .**
  - Operate across markets, sectors, 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.

-  **The ways to reduce risk of fraud is to . . .**
  - Create your own customer/supplier/payee profiles.
  - Validate all new/change beneficiary requests with a phone call to a number on file.
  - Confirm agreements in writing and with a phone call to known contacts.
  - Never deal with agreements from unknown requesters.
  - Implement a robust process for adding/changing beneficiary information.
  - Ensure beneficiary payment processes are robust, preferably involving a checker.
  - Always be vigilant to requests that contain red flags.

### Best Practices

#### Actions to protect your organization

- 
  - **PERFORM checks to reduce fraud risk.**
    - » Validate payment instructions for any new counterparty, the same authentication should be applied for any subsequent change requests received.
  - **MANAGE high-risk transactions.**
    - » Configure your systems to require dual approval for high risk activity.
  - **REDUCE business-wide transaction risk.**
    - » Segregate duties for sensitive and high-risk activities.
  - **UNDERSTAND social engineering.**
    - » Promote training on cyber threats/fraud awareness.
  - **CHECK user activity.**
    - » Regularly review your transaction reports.

**IF YOU ARE A VICTIM OF AN ATTACK, CONTACT YOUR SECURITY OFFICER AND YOUR REGULAR CITI CONTACT. CITI HAS A FRAUD INVESTIGATION SERVICE THAT IS FULLY TRAINED TO INVESTIGATE AND MANAGE FRAUD ATTACKS.**