Guidance on How to Combat Fraud

Red Flags

For email, letter, phone, transaction and systems comms

How do you know the email, telephone, letter you have received requesting information or instructing a transaction is not fraudulent? Confidence tricks that exploit human psychology and other engineering tactics play heavily in an attempt to commit fraud. Be vigilant: recognising tells and asks is the most effective reflex to combat fraud.

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
- Senior officer name-dropping to rush transactions

- Poorly written grammar, syntax or spelling
- Fake letterhead, faxed or email instructions
- Contacts or details not the same as the bank's
- Email address variations or domain name changes

- Customers/suppliers calling in before callbacks can be made
- Changes in a customer's/supplier's usual callback number
- Customers/suppliers are rarely available via official channels
- Customers/suppliers seem anxious to complete transactions

- Customers/suppliers contact details that aren't on file
- 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 alleged customers on unusual numbers
- Give a password in a place you do not recognise
- Accept enclosed or unconfirmed contact details
- Receive or act on unsolicited instructions
- Click on unexpected, unfamiliar or fake links

- Circumvent procedures with plausible reasons
- Deal with a first-time or unknown beneficiary
- Provide SWIFT payment confirmation by email
- Carry out instructions after a profile change
- Make immediate or urgent payment changes
- Remove close to all or an entire account balance

- Approve an unknown or unfamiliar transaction
- Transfer funds by or before an extended holiday
- Transfer funds to a known secrecy haven
- Transfer a small followed by a large sum to a beneficiary
- Transfer funds to an alternative jurisdiction

Do's and Don'ts

For devices (smartphones, tablets, laptops and pcs)

To effectively adopt these recommended practices, you may need to involve your IT department. This may require that you undergo a risk assessment in compliance with their own controls and evaluations.

Do . . .

- ✓ Use anti-virus, -spyware or -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 using CitiDirect BE℠.
- ✓ Keep your Java plug-in updated so that software runs smoothly and as expected.
- ✓ Password-protect any devices that you use to access your CitiDirect BE℠ platform.
- ✓ 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.

Do not . . .

- ✗ Use your computer without anti-virus, anti-spyware or -malware detection software.
- ✗ Install applications or software from unknown sources or companies you do not trust.
- ✗ Use technology without a native or third-party pop-upblocker to defend against malware.
- ✗ Leave your browser window open on devices after you have finished using CitiDirect BE℠.
- ✗ Use a device or computer without the most recent or updated version of the Java plug-in.
- ✗ Access CitiDirect BE℠ 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 unexpected email links.
- ✗ Share PC screens with any unauthorised person.

Risks and Controls

For beneficiary change requests

Recognising 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 problems 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 new 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.
- Independently validate all change requests that you receive.
- Confirm agreements in writing with known contacts.
- Never deal with agreements from unknown requesters.
- Validate only via approved channels and contacts.
- Ensure beneficiary payment processes are robust.
- Always be vigilant to unusual or requests that contain red flags.

Best Practices

Actions to protect your organisation

- You want to **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.
- You want to **MANAGE** High-value or -risk transactions
  - » Set additional approval levels in CitiDirect BE℠ maker/checker.
- You want to **REDUCE** business-wide transaction risk
  - » Segregate duties for sensitive and high-risk activities.
- You want to better **UNDERSTAND** social engineering
  - » Promote training on cyber threats/fraud awareness.
- You want to know how to **CHECK** user activity
  - » Regularly review your transaction reports and dashboards and conduct frequent user audits.
- Complete the Citi 'Social Engineering' Fraud Awareness training available at **http://www.citibank.com/tts/sa/emea_marketing/training/index.html**

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.