Commercial Bank

Beneficiary Change Request Fraud Alert:

Payments fraud across markets and industries has been increasing very rapidly over the past year. Fraudsters are becoming more creative and more sophisticated.

For example, fraudsters may attempt to redirect payments by requesting that you change the beneficiary information of a longtime supplier. Fraudsters may also obtain or forge supplier letterhead and send you a notification of a purported bank change or bank account number via email, or they may pose as a new account manager and subsequently request similar changes in banking details.

Citi recommends that each client review its company's internal procedures for dealing with any requests to change beneficiary payment details.

Examples of Good Practices:

- Create your own customer/supplier/payee profile
- Independently validate changes requested with an established/ approved contact to verify what is being asked
- Confirm all payment requests with an outbound phone call to a contact at a phone number you already have on file (never use the contact information contained in the request)
- Implement a maker/checker process to verify all payment requests

Examples of Red Flags to be aware of:

- Slight variations in email address and/or domain. (example: **name@domain.com** and **name@domain.net** – creating another domain name ending in .net instead of .com)
- Requests to only contact suppliers via the phone numbers or contact information on recently received correspondence
- Requests for immediate, urgent payment changes with plausible reasons for not being able to comply with usual authorization or related procedures
- Be wary of inbound phone calls from individuals following a payment change request made via email

Please share this important information with other colleagues at your company.

1460635 08/16