Treasury and Trade Solutions

Beneficiary Change Request Fraud Alert:

Fraud across all markets and industries is increasing. Fraudsters are becoming more creative and sophisticated. We are aware of increased attempts by fraudsters to redirect payments from existing payment instructions by fraudulently changing the beneficiary bank details. Fraudsters may get hold of or forge supplier letterhead and send you a notification of a bank change or they may pose as a new account manager, and subsequently request changes in banking details. Approaches are ever changing.

We ask that you review your own internal process regarding any requests made of you to make changes to the payment details of the beneficiary party.

Good Practices include (and this is not an exhaustive list):

- Create your own customer/ supplier/ payee profile
- Validate all change requests received
- Independently validate changes requested with an established/approved contact to verify what is being asked
- Confirm in writing to an established contact what has been agreed (not to the requester if requester is different)

Red Flags to be aware of include:

- Slight variations in email address and/ or domain. (Spoofing is where genuine email addresses can be replicated)
- Requests to only contact suppliers via the numbers or contacts on received correspondence
- Requests for immediate, urgent payment changes with plausible reasons for not being able to comply with usual amendment procedures

Remain vigilant.