London 05 September 2019

Social Engineering Fraud Awareness
Reminder for all employees

Dear all,

In the modern business environment companies are increasingly exposed to ever more imaginative methods fraud, whilst Finance colleagues need to be on front end of the fight against this risk, all Colart employees play a part in mitigation and we all need to remain vigilant in combatting this potential threat.

Fraud arising from social engineering presents is a real threat. Whilst many approaches adopted by fraudsters utilise technology it is often enabled as a result of human interaction. It is important we are all aware of the potential for psychological manipulation of our people to perform actions or divulge confidential information, and the actions we can all take to mitigate the threat.

- All employees must be aware of these threats and familiarise themselves with the following
- Finance and supply chain employees are required to ensure detection/prevention controls are applied to all local processes.

Invoice fraud
Requests received purporting to be from a Colart supplier/customer requesting amendments to bank details/addresses with the objective of illicitly receiving funds/goods

How can we protect our business?

- Has the request been received from a recognised and verified contact?
- Genuine email chains can be intercepted and altered – remain vigilant
- Verify the request with a pre-existing contact by telephone
- Use single points of contact with key suppliers/customers to minimise uncertainty
- All amendments to any details should be subject to dual controls
- Raise any suspicions with internal management (Financial Director for respective business unit)
- If in doubt – do not make payment

Email fraud
Instructions received imitating senior management advising immediate payment is required.

How can we protect our business?

- Identify authenticity. Is this a Colart email address?
- If the address is right – is the spelling, tone or grammar unusual?
- All payments should operate on a purchase order basis. Individual payment instructions from our CEO/GLT are extremely exceptional and cannot by-pass or super seed the existing approval matrix structure
- Verify the request with the originator (via a verified contact address)
- Protect information. Be cautious of the amount of business-related information you reveal – this can enable fraudsters

- All payments should be subject to dual approval
- If in any doubt – do not make payment
- Do not respond/forward the email (to protect against spreading possible viruses) but ensure your business unit Financial Director is informed of any suspicious emails

Phishing, vishing and smishing
The attempt by fraudsters to attain sensitive information via the use technology (email, telephone and SMS)

How can we protect our business?

- Be suspicious of callers with an urgent/forceful tone
- Terminate any suspicious calls and call back on a verified and pre-known number
- Do not dial back to the number you received the call from – this alone can be a scam
- Do not divulge sensitive information without clear justification and approval. If in doubt – don't share anything
- Check the location of link (roll your mouse over to reveal the true location of the link or are there missing/extra characters
- Remain sceptical of unexpected emails or unknown sources – do not open links or attachments unless verified
- Inform your respective business unit Financial Director of any suspicious interactions

Additional guidance:

- Take Five – Stop Fraud
- Barclays Digital Wings
- Chubb Insurance