CASE STUDY - FRAUD ON TIME-CRITICAL PROCUREMENT (COVID-19)

Fraudsters use a wide variety of tactics to defraud institutions, sourcing time-critical, scarce goods for medical/health purposes, including mimicry of existing suppliers or creation of new artificial vendor firms.



Fraudster Preparation

Fraudsters research the buyer institution and identify the key buyer contact details and a reputable supplier which they will impersonate or set-up as a fake new vendor.

Best Practice

 Roll-out regular cyber security/social engineering training for all staff – even apparently innocuous information can facilitate fraud



Initial Contact and Offer

By impersonating a reputable supplier or posing as a new vendor, fraudsters engage with key buyers (via phone/email) and promise an unusually large supply of scarce goods if buyer acts quickly.

Best Practice

- Beware of, and check for, email spoofing
- Be wary of offers which appear 'too good to be true' i.e. quantity and/or pricing that seems unrealistic in the current market conditions
- Increase vigilance if time urgency is imposed
- Increase vigilance if supplier has minimal product knowledge
- Do not accept unverifiable references

3



Order Capture

Fraudsters may create a clone of a supplier website or a fraudulent website to give additional credibility.

Fraudsters send an email containing a link to fraudulent site. The buyer then places an 'order', either directly on the website or via fraudulent contact details provided (email, fax, phone).

Best Practice

- Validate any recently registered companies with no previous verifiable trading history or companies whose business activities are inconsistent with goods being sourced
- Be wary of any emails with embedded url links



Fulfilment and Payment Demand

Fraudster confirms the 'order', and advises that due to scale and context

- 1. Fulfillment will be via a totally new 3rd party intermediary, and;
- 2. Substantial downpayment is required prior to goods inspection to secure 'order'.

Best Practice

- Undertake full due diligence for all new commercial counterparties
- Be suspicious of any contract that contains unusual terminology



Fraud Discovery

Buyer instructs a down-payment to the fraudsters account

Buyer attends an inspection, no goods present

Buyer inquires at reputable supplier or digs into new vendor details and realizes this is fraud

Best Practice

- Beware of new account details for an existing counterparty – particularly with large value payments
- Be vigilant to sudden beneficiary account change requests



Urgent Response

Buyer immediately contacts his bank and law enforcement to report fraud

Though fraudster has rapidly moved funds to remote jurisdictions, banks endeavour to freeze/return funds.

Best Practice

 Engage bank and law enforcement urgently
– speed of report and probability of funds return

are positively correlated

