POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Procurement Fraud Advice

The ability to detect a fictitious company and business transaction in a period of high demand becomes more challenging, particularly where businesses are operating with a skeleton or remote workforce. Many businesses are establishing new supply chains for products, particularly personal protective equipment (PPE) and buying from companies they have not dealt with before.

This provides fraudsters an opportunity to exploit the situation: high demand for and the urgency with which companies want to procure goods. Those conducting this type of fraud will often target individuals/companies, knowing that they are facing these challenges.

At this time the care sector and other businesses needing to procure PPE and other essential goods are particularly vulnerable and the fraudsters know this.

In amongst all the strain of responding to the challenges and demands of COVID-19, businesses are urged to maintain as much normal rigour as possible in their internal systems and processes, safety practices and physical and cyber security.

To help prevent procurement fraud:

Top 10 Tips

1. Ensure all staff who are able to make or are involved in financial decisions are trained how to identify procurement fraud.

2. Never give in to pressure or threats that it is a time-sensitive issue or an urgent matter. A genuine organisation will have no issues with you verifying a request, however a fraudster will often try to pressurise you into acting immediately.

3. Ensure a three-way match is carried out. Do the amounts documented on the requisition, purchase order and invoice all align?

4. Adopt dual control procedures for authorising payments. Ensure that a senior member of your team reviews your actions and formally authorises the payment.

5. Ensure the procurement process is followed and is enforced. Has an order been placed before the procurement paperwork has been raised? If so, why?
6. Carefully check the sender's email address to identify if it exactly matches your known and trusted records and call your supplier to verify the email is genuine.
7. Be vigilant to any clerical or spelling errors within emails which may indicate the email is fraudulent'.
9. If it is a new supplier, carry out internet searches to check if they are genuine, are there any customer reviews and phone any listed landline to check.
10. Be alert to any requests to alter bank details. Carry out an internet search of the new bank account sort code and account details to uncover: Location of the bank (to be checked against the company address) and whether there are any blogs or reports available to indicate the communication is a scam.

If you think you have been scammed, report it to your bank immediately.

To report a crime, call Action Fraud on 0300 123 2040 or if you live in Scotland, report to Police Scotland on 101 or 999 in an emergency

For help and advice on scams please contact Citizens Advice on 0344 411 1444 or if you live in Scotland, Advice Direct Scotland 0808 164 6000

Further information on preventing fraud can be found at

https://takefive-stopfraud.org.uk/

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Special thanks for this publication to Police Scotland