FRAUD ADVISORY PANEL

COVID-19 Fraud Watch

THURSDAY 11 JUNE 2020

CURRENT COVID-19 FRAUD RISKS

- Fake websites impersonating UK retailers (esp. UK supermarkets and Amazon)
- Impersonation of NHS test and trace service
- Procurement fraud
- Government stimulus schemes and universal credit (esp. BBL, SBGF, RHLGF)
- Insider fraud (esp. hours, payroll, recruitment)
- Phishing emails (esp. Office365, HMRC, debt management companies and PPE)
- Funeral costs (bereavement) fraud
- Changes in business purposes and type of goods sold (to PPE, face masks etc)
- Doorstep crimes
- Tenancy fraud.

ANTICIPATED AND/OR EMERGING ISSUES

- Fraudsters are modifying their approach to invoice fraud by asking businesses to change the beneficiary account details to circumvent the new confirmation of payee process.
- From Asia it has been suggested that there might be an increase of exports of chemicals required to make synthetic drugs/narcotics or materials used to refine opium as small factories begin to resume production and shipment.
- A criminal group has been identified which appears to be intercepting one-time passwords using an automated telephone service (which calls victims to ask them what their one-time password is).

SOME SIMPLE PREVENTATIVE TIPS …

- Bank customers should always perform independent due diligence checks on any requests received to change bank account names and numbers.
- It is more important than ever for organisations to encourage their people to do the right thing and to perform periodic checks and balances to prevent, detect and deter fraud.
- The Ministry of Housing, Communities and Local Government has published a review into the risks of fraud and corruption in local government procurement, available here.
- CIPFA have produced a webinar on COVID-19: fraud risks and the government's response, available here.
- The NHS Counter Fraud Authority have produced prevention advice and guidance, available here.
- The ICO has developed a data protection and coronavirus information hub, available here.