FRAUD ADVISORY PANEL

COVID-19 Fraud Watch

THURSDAY 09 JULY 2020

CURRENT COVID-19 FRAUD RISKS

- Fraudulent automated calls (esp. impersonation of Amazon and financial services)
- Online shopping and auction fraud
- Dating fraud
- Investment fraud (esp. cryptocurrency)
- Courier fraud
- Phishing (esp. impersonation of HMRC and financial services)
- Account takeover fraud.

ANTICIPATED AND/OR EMERGING ISSUES

- Financial services firms are seeing quite widespread evidence of government grants, particularly BBLS, being exploited with a high level of sophistication by both OCGs and individuals.
- Use of multichannel attacks against organisations by fraudsters.
- Fraudsters have been paying young adults for their personal details. They then use the information to form companies, open bank accounts, and register with HMRC.
- A recent survey by Netwrix revealed that inappropriate data sharing continues to be a problem for companies and businesses.

SOME SIMPLE PREVENTATIVE TIPS …

- Testing is important in the current environment, particularly the testing of staff, internal controls, systems and processes.
- It is important to assess and be alert to the vulnerabilities and risks associated with new channel requests from customers.
- Regularly monitoring user data access privileges will make it easier to track data sharing within an organisation.
- Organisations concerned about the security of their customer/supplier/membership databases should read the advice and guidance available from the ICO, available here.
- Action fraud regularly release prevention information on Twitter, available here.
- You can report phishing emails to the National Cyber Security Centre by forwarding the email to report@phishing.gov.uk.