FRAUD ADVISORY PANEL

COVID-19 Fraud Watch

THURSDAY 23 JULY 2020

CURRENT COVID-19 FRAUD RISKS

- Business impersonation fraud (esp. on social media platforms)
- Data breaches (esp. affecting third parties such as CRM providers)
- Fake social media profiles and adverts
- Cloned websites
- Targeted malware attacks
- Mandate fraud
- Fake ATOL and ABTA invoices

ANTICIPATED AND/OR EMERGING ISSUES

- A new risk has been identified associated with the bounce back loan scheme where directors change their details.
- Concerns were voiced about the use of virtual offices and PO boxes which enable people to easily set up and trade with an air of legitimacy, often without any proper anti-money laundering checks being performed.
- Researchers from Ben-Gurion University (BGU) have found that image processing algorithms and web-based text recognition meant they could identify personal features such as gender, age, and usernames. This could pose a risk to the privacy and security of users.

SOME SIMPLE PREVENTATIVE TIPS …

- The NCSC has revised its advice on how to manage the presence of high risk vendors (HRVs) in the UK's telecommunications networks, available here.
- The NCSC has published guidance on how to use video conferencing platforms securely, available here.
- Organisations concerned about the security of their customer/supplier/membership databases should read the advice and guidance available from the ICO, available here.
- You can report fake adverts to the Advertising Standards Authority here.