FRAUD ADVISORY PANEL

COVID-19 Fraud Watch

CURRENT COVID-19 FRAUD RISKS

- Procurement fraud (esp. PPE equipment from overseas)
- Benefit fraud (including phishing emails and fake claims)
- Online shopping fraud (esp. fake medical goods)
- Impersonation of HMRC, DWP, FCO and travel companies
- Fake applications for government support/grants
- Payment diversion fraud
- Fake online communication sites (esp. including domains using 'Zoom')
- Authorised push payment fraud
- Charity impersonation fraud
- Romance fraud.

ANTICIPATED AND/OR EMERGING ISSUES

- Social engineering techniques adapting to focus on COVID-19
- Fake charities or businesses being set up to access grants/support
- Hacking and DDOS attacks
- Ransomware targeting the health sector and social services.

SOME SIMPLE PREVENTATIVE TIPS …

- Monitor the global situation closely. There have already been various reports of an increased threat from cyber attacks targeting healthcare (hospitals) and social services.
- Implement additional verification procedures before making payments to reduce the risk of payment diversion fraud. For example, by using Skype.
- Report fraud to Action Fraud.
- Consider the adoption of the free www.quad9.net tool which blocks 60m cybercrime events daily and has included a relevant subset of these 20,000 domains.
- Use the Global Cyber Alliance's 'working from home' toolkit.
- Read and act upon the National Cyber Security Centre (NCSC) guidance for business on:
    - 10 steps to cyber security
    - Working from home and how to spot fake coronavirus emails,
    - Allowing staff to use their own devices to work remotely, and
    - How to deal with suspicious emails and messages.

Also see: The Thomson Reuters Practical Law free business crime and investigations (England and Wales) tracker on the COVID-19 outbreak.