Grant Thornton
An instinct for growth™

Anti-Fraud Coronavirus Article – 15/04/2020

Covid-19	**Fraudsters continuing to exploit the Coronavirus situation**

Times of crisis are, unfortunately, moments when organisations and people are most distracted or impressionable. We have seen this with the Covid-19 (Coronavirus) which is continuing to cause worldwide disruption which provides fraudsters with the opportunity to exploit and steal.

Your Counter Fraud team are still available to help with any concerns or issues you may wish to report during this period of disrupted working. It is important now, more than ever, that we remain vigilant, don't let our guard down and lock down anything that maybe vulnerable. Most importantly, we don't allow ourselves or **OUR NHS** to fall victim to fraudulent activity.

The Covid-19 Fraud Watch Group* latest identified fraud risks

General

- Increase in whistleblowing reports (esp. employee conduct and health and safety)
- Data breaches relating to remote working/customer information
- Fraudsters offering cleaning services to protect from COVID-19
- Pension liberation fraud
- Financial investment fraud
- Increase in grant applications from fake businesses

Fraudulent websites

- Free of charge DBS checks subject to a 'low cost' admin fee
- Access to 'free' COVID-19 webinars subject to providing personal/administrator details

Phishing emails

- Targeting parents/carers offering free school meals for their children subject to providing their bank details
- Targeting professional firms from the 'Commonwealth Unit' asking for an advance fee of £2500 to become the sole practitioner on a new 'Parliament Hub App'
- Offering 'free' help in order to obtain system access (e.g. website development)
- Advising that the recipient's mailbox is full but that they can increase their storage space free of charge by clicking on the link provided

Anticipated and/or emerging issues

- Hospitals targeted by ransomware because of vulnerabilities in their VPN and network gateway devices
- Donation pages automatically set up for businesses without their knowledge or consent

- South Africa has seen an increase in courier fraud with fraudsters claiming that all money is contaminated with the coronavirus and they will collect it
- Private Branch Exchange (PBX) fraud where fraudsters hack the telephone system to make expensive calls
- Fake recruitment agencies offering to provide temporary workers

* With thanks to the Fraud Advisory Panel, Covid-19 Fraud Watch Group which consists of cross-sector and industry members including the Cabinet Office and City of London Police.

OUR ADVICE

✓ **Some simple preventative tips ...**

- Read the little booklet of phone scams from the Met Police.
- 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
  - How to deal with suspicious emails and messages, and
  - Stay up to date with the latest trends by accessing the NCSC's weekly threat update.
- Use the Global Cyber Alliance free resources:
  - www.quad9.net
  - DMARC
  - Working from home toolkit

If in doubt – Report It!

We are here for you - for advice or training on anti-fraud matters, please contact your Local Counter Fraud Specialist

Sarah Kabirat, Local Counter Fraud Specialist
Landline: 020 7383 5100
Mobile: 07927 721625
Email: sarah.kabirat@uk.gt.com or Bcpft.fraud@nhs.net

You can also report your suspicions directly to the NHS Counter Fraud Authority via:

NHS Fraud and Corruption Reporting Line (Powered by Crimestoppers):
0800 028 40 60
On-line: www.reportnhsfraud.nhs.uk

PROTECTING THE NHS FROM FRAUDSTERS