COVID-19 Fraud & Security Alerts

Ref: CFMG-004

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Government Counter Fraud Function – bank account verification and active company checks

The Government's Counter Fraud Function has worked in partnership with Experian to introduce two new complementary products to assist public bodies in dispersing funds for the COVID-19 Financial Support Schemes. For the first time, public bodies can now verify the bank accounts of limited companies, sole traders and charities electronically using data from nine major UK banks.

Verifying that a bank account belongs to a business or individual helps to mitigate the risk that funds are paid to incorrect or fraudulent accounts. Experian's Bank Wizard Absolute solution aims to verify the ownership of the account by matching the account details provided by the client (e.g. a local authority) with the details Experian holds on behalf of the banks. This provides increased confidence that funds are being paid to the right account. For simplicity, the service has been configured to return a 1-8 risk flag based on the status of the account match. The granular flags and scores are also returned to aid investigation or follow-up. The solution covers an estimated 75%+ of valid UK payment accounts.

In addition, the Counter Fraud Function and Experian have also developed an active company check that can be used to verify if a company exists and is actively trading. Verifying that a business is who they say they are and is actively trading helps to ensure that grants are allocated to the right businesses whilst reducing the risk of fraud and error. The Active Company Check solution makes it quicker and easier for you to verify the existence of a business based on a number of corroborated commercial data sources. This provides increased confidence that the details you have been provided with are accurate, and that the company is active. For simplicity, the service has been configured to return a 1-10 risk flag to help determine if the company is actively trading. This information should be taken into consideration to help expedite payments to eligible businesses. Metadata is also provided to assist you with your upfront and post-event assurance checks.

NHS Counter Fraud Authority (CFA) COVID-19 fraud threat assessment

A thematic assessment on 'Fraud threats to the NHS from COVID-19' is now available on the CFA Extranet. The aim of this threat assessment is to inform the counter fraud community of the identified threats that may impact on their area. This is the first of several threat updates to be compiled and released. The threat assessment was collated from information obtained from open source research, other law enforcement and

intelligence agencies. Fraud referrals from members of the public and Local Counter Fraud Specialists (LCFS) were also analysed, assessed and evaluated. Click here to access the assessment

CLUE update

CLUE is a new case management system which will replace FIRST across the NHS and will contain existing investigation and intelligence data, currently held in FIRST. Recently CLUE has been implemented into the NHSCFA and NHS England (NHSE) and is now operational. A bespoke training package has been developed for LCFS by NHSCFA and NHSE. The implantation of CLUE is currently in phase 2, involving the on-boarding of the Department of Health and Social Care, larger Special Health Authorities, and Counter Fraud Services Wales over a three month period. This is in order to easily identify and rectify issues from these organisations, due to their centralised structure and high reporting volumes. Due to delays caused by COVID-19, timescales to continue on-boarding cannot be confirmed. The very earliest that training on CLUE could resume would be Q3 2020/21. The remaining LCFS training would not start until 3 months after the phase 2 training begins.

COVID-19 Crown Prosecution Service protocols and guidance

Updated guidance and protocols have been produced by the CPS to address changes made as a result of the COVID-19 pandemic. Due to safety measures to protect public safety, best practice guidance has been provided for statement talking over the telephone. This guidance covers the requirements of digital signatures and other best practice tips. Click here to view the CPS best practice guidance

Guidance has been drawn up between CPS, National Police Chiefs' Council, The Law Society, Criminal Law Solicitors Association and London County Courts Solicitors Association regarding interviews under caution and court proceedings in the current circumstances. In addition, the CPS and NPCC have issued interim charging protocols for the COVID-19 crisis. Click here to read the interim charging protocol Click here to read the interview protocol

COVID-19 home antibody test deliveries halted

Professor Stephen Powis, Medical Director at NHSE, issued a warning last week against the use of antibody tests sold by retailers. Following this, it was announced on Wednesday 27 May that the Medicines and Healthcare Products Regulatory Authority has now contacted all private providers and labs to halt the tests, whilst a review of their accuracy is completed. Professor John Newton of Public Health England (PHE) stated; "*We wouldn't recommend at the moment that people rely on the tests that are becoming widely available. My advice would be to wait until we have better tests which will be available in a similar form very soon, though they are still under evaluation at the moment.*"

It has also been reported that some online retailers providing COVID-19 home antibody testing kits have falsely claimed they are endorsed by Public Health England. One company was reported to PHE and the company has dropped the endorsement claim from advertising material.

Click here to read more about NHSE's home testing warning

Click here to read more about the halt to COVID-19 home testing

Cervical screening text scam

A text scam claiming to be from Public Health England states recipients are overdue a cervical screening text. The text states the recipient should call a mobile number and confirm personal details. It has been confirmed these messages are not from the NHS Cervical Screening Programme and the case has been passed to Action Fraud.

NHS text scam

Text scams attempting to gain personal and financial details have continued to circulate. A recent example includes the message 'As part of the NHS promise to battle the COV-19 virus, HMRC has issued a payment of £258 as a goodwill payment.' The message contains a website link which uses UK government branding, in an attempt to obtain personal data.

Mandate fraud attempt of NHS supplier

A mandate fraud attempt has been reported linked to a NHS organisations supplier. Financial Data Management (FDM). A client's email account was compromised. They received an email purporting to come from the FDM accounts division, fraudulently advising them of a change in bank details.

Free webinar – how to plan and prepare for a cyber event

A free webinar will be held on Monday 1 June covering how businesses and organisations can plan and prepare for cyber incidents. The webinar will cover planning, identifying common gaps and learning outcomes. The event will be run by West Midlands Police and Tarian (a Welsh organised crime unit) cybercrime teams. It will be held on Monday 1 June 2020 at 14:00 – 15:00.

Click here for more information and to register

Other type of fraud examples

Email scams & Phishing scams

- Due to widespread cancelations to holidays and travel due to the pandemic, reports of holiday related scams continue to rise. These scams often use emails purporting to be from a travel company, requiring the victims to supply personal and financial details to speed up refund claims. Recently a large number of scams have been focused around cruise refunds and Future Cruise Credits.
- Emails purportedly from BMW (car manufacturer) inform recipients they have won a BMW 5 Series, along with a cash price in a COVID-19 lottery. The email claims the recipient is required to contact the claims department and send personal details to claim the prize.
- Businesses including Lloyds Pharmacy, Greggs, Boots, and Marstons Brewery have been targeted by emails attempting to acquire information which would support fraudulent applications for COVID-19 grants. The emails use the closure of premises and homeworking to justify the contact. The sender's email address on these communications is not correctly formatted and website links and telephone numbers are incorrect.

- As previously reported in our weekly alerts, TV Licensing scams are continuing to be reported to Action Fraud.
- Domino's Pizza has confirmed this week a scam offer has been identified. Text and WhatsApp messages have been used to circulate the offer stating 'Dominos is giving away 2 FREE Large Pizzas per family to everyone this week to support the nation during Corona Pandemic'. A link contained in the message prompts customers to enter personal and payment details.

Online Retailers / Counterfeit goods

- Warnings continue to circulate on fake personal protective equipment, mainly facemasks. Many reports focus on Chinese standard rated KN95 face masks, which are not permitted for use in the UK market. An investigation has been launched by the Australian Health Ministry to address how counterfeit facemasks were supplied to hospitals.

Social media and other messaging platforms

- Romance scams have increased during the pandemic, as criminals exploit loneliness. Scammers create a fake identity to enter into a relationship with a victim with the intent to steal either funds or personal information. In some cases romance scams can lead to sextortion, were the victim is encouraged to send indecent images. The fraudster then threatens to share the images unless a financial payment is made.
- Promotions for a fake free food voucher for Lidl have been identified on social medical platforms Twitter and Facebook as well as messaging service WhatsApp. The messages state vouchers of up to £175 are available for food retailer Lidl, to support customers during the pandemic. A link is contained within the messaging, taking victims to a spoof site to gain personal details.
- WhatsApp users have reported messages purporting to be from the WhatsApp technical team which require the recipient to share verification codes. These codes are used to verify the account on a new device. The messages use company branding to appear genuine.

Software

- Users of the QTS operating system (used in file sharing, data storage and back up) have been urged to update to the latest version of the platform. Older versions can be vulnerable to attacks which could result in allowing remote access.