COVID-19 risk briefing

Covid-19 is creating exceptional circumstances and while the country adjusts to life under lockdown, criminals are identifying ways to exploit the vulnerable at this time of uncertainty.

In this risk briefing, we have summarised some of the key fraud trends and cases we have identified through the information and intelligence we receive via law enforcement as well as through our own open source research.

We have also identified some red flag indicators for the ways in which criminals may seek to use the Covid-19 crisis to launder money.

Fraud trends

The UKFIU has published a guidance note on COVID-19 that sets out observations from SARs Reporting. They have also set out new Glossary Codes in relation to any COVID-19 suspicions, fraudulent use of Government Priority Schemes and fraudulent use of the HMRC Self-Assessment Tax Refunds system.

The press have covered a number of stories around the following areas:

- Increase in new companies registered on Companies house with either COVID-19 or Coronavirus in the title.
- Individuals impersonating the government, or HMRC, notifying the victim that they were due a rebate and requesting bank details to enable the payment.
- The elderly continue to be targeted by fraudsters. The National Fraud Intelligence Bureau have received over 500 reports with approx. losses of £1.6m
- Criminals are using scare-tactics to pressurise investors to move their investments – they claim that the pandemic provides time-critical opportunities. Information around the investment opportunity is often sparse.
- Bogus companies are purporting to sell faces masks, hand sanitiser and other PPE but once the payment is made, the company disappears.
- ICAEW reported in ICAEW Daily that online fraudsters have sent phishing emails targeting unsuspecting businesses claiming to be from HMRC chief executive, Jim Harra.
- Social engineering whereby fraudsters impersonating high street banks persuade their victims to transfer funds to a new account following a ‘security breach’ and a change to normal procedures as a result of COVID-19. Social engineering is where the fraudster has researched a particular victim via their social media accounts and other sources.
- Bogus emails asking for a donation to tackle COVID-19, normally pretending to be from a charity which is assisting vulnerable people during the outbreak.

Red flag indicators during Covid-19

Firms should be aware of certain risk indicators that may lead to concerns that a client is vulnerable to fraud, bearing in mind the emerging fraud and criminality trends.

Risk indicators for money laundering may include:

- Income from services/sectors that should have halted trading during lockdown (eg, nightclubs, pubs, restaurants, taxi and travel businesses).
- Unexpected or unexplained large receipts into bank accounts, which the client explains as funds from a planned holiday, house or car purchase, cancelled due to COVID-19.

Firms should also be particularly alert to the following risks in new or prospective customers:

- Claims that a new client can't provide any form of identity verification evidence, or pressure to forego necessary due diligence checks to 'speed up' the process.
- Being asked to work with unusual types of client or on unusual types of matter, of which the firm has little experience
- Becoming involved in work that is outside the firm's normal area of experience/expertise – without full understanding of the money laundering and counter terrorism risks associated with the new area of work
- Transactions where the business rationale for the transaction is not clear.
- Requests to access client accounts but with no associated request for accountancy services.

Useful resources

If you know/suspect money laundering or terrorist finance activity you should make a SAR submitted to the NCA under Part 7 Proceeds of Crime Act 2007 and the Terrorism Act 2000. Guidance on making SARs is available at nationalcrimeagency.gov.uk.

Coronavirus: Guide to client due diligence

ICAEW's Business Law Department has issued a guide on how to adapt client take-on procedures to reflect more remote interactions with clients. Download the guide

ICAEW coronavirus hub

icaew.com/coronavirus

ICAEW Technical and ethics support

Contact ICAEW's Technical and ethics support team by emailing: technicalenquiries@icaew.com or via web chat at icaew.com/webchat

Action Fraud

actionfraud.police.uk

Reporting suspicious emails

Report suspicious messages to the National Cyber Security Centre
Forward suspicious emails claiming to be from HMRC to phishing@hmrc.go.uk and texts to 60599.

Cyber security

It is as important as ever that you have good procedures in place to ensure you receive and share data securely. Read ICAEW's insights on how to keep your IT systems and networks safe. Visit icaew.com/cybersecurity