COVID-19

Suspicious Activity Reporting

This document aims to provide reporters with observations from the UKFIU on what is being seen in reporting around COVID-19 and SARs.

April 2020

v1.0

This is a United Kingdom Financial Intelligence Unit (UKFIU) Guidance Note. It is produced in line with the National Crime Agency (NCA) commitment to share perspectives on the Suspicious Activity Reports (SARs) regime.
Trends/observables

Money laundering

Several SARs have been seen relating to suspicions that individuals are exploiting the COVID-19 outbreak to account for money movements that suggest possible money laundering. COVID-19 is resulting in the general public making a lot of changes to their behaviour. Most of these are not suspicious; however, in the below examples reporters have cited some of these in combination with other money laundering red flags.

- Large credits or cash deposits into accounts, which the account owner explains as funds from a planned holiday, house or car purchase, cancelled due to COVID-19 (sometimes into previously inactive accounts) or business owners claiming to be making deposits for staff wages.
- Sending funds abroad to relatives to buy face masks.
- Customer claim funds, received into accounts from multiple sources, from the importation and selling of face masks.
- Customers in receipt of multiple faster payments then withdrawing large amounts in cash, claiming to have lost faith in the banking system as a result of COVID-19.
- Concerns around the issue of facilitating ‘emergency’ loans to subjects about whom they hold money laundering concerns.

Fraud

SARs have reflected how the COVID-19 pandemic is being exploited to further facilitate existing fraud methodologies. Examples include:

- Individuals or businesses suspected of taking payment for, but not supplying, face masks, hand sanitisers and other Personal Protective Equipment (PPE).
- Social engineering whereby fraudsters impersonating high street banks persuade their victims to transfer funds to a new account following a ‘security breach’. The fraudsters used COVID-19 as an excuse for changes to normal bank procedures.
- Victims believing they are investing in companies developing a vaccine for COVID-19.
- Refunds claimed for fake bookings cancelled due to COVID-19.
- Suspicions that an individual suddenly moving funds from a savings account could be an attempt to the hide true value of savings, in order to fraudulently claim government compensation for loss of earnings.