COVID-19 (Corona Virus) Financial Crime Risk Bulletin

April 2020

By Financial Crime Compliance (FCC)

Introduction

In **March**, we reported on the unprecedented opportunities, created by the COVID-19 pandemic, for fraudsters and cyber-savvy criminals to target the funds and data of private individuals, employees and businesses, including Standard Chartered. This bulletin updates on how the threats we identified appear to be impacting the bank, our clients and our customers. It also updates on the actions Standard Chartered is taking to collaborate internally and externally with partner agencies, peer banks and law enforcement, to exchange intelligence that can be used to mitigate the cyber and financial fraud threats we are all facing.

SUMMARY

- **Financial Fraud** and **Cyber Crime** campaigns remain the most common COVID-19-related financial crime activities detected and reported to date.
- The pandemic appears to be enabling the illicit markets for counterfeit goods, pharmaceuticals, and may be enabling the misappropriation of government aid or healthcare-related funds by **corrupt officials**.
- The pandemic appears to be disrupting supply and demand for various illegal drugs trades, and the operations of Human Trafficking and Modern Slavery criminal networks.

What are the criminals doing?

Most of the reported financial frauds are COVID-19 themed variations of known scam methods targeting individuals or companies to steal funds:

- **Fake investments** e.g. COVID-19 related goods and services, crypto assets and currencies.
- **Fake companies** e.g. posing as suppliers of ventilators or Protective Personal Equipment (PPE); mis-selling medical support services, or selling counterfeit products to medical centres and the public, e.g. face masks
- **Fake charity fundraising schemes** e.g. raising money for COVID-19 causes where funds are then misappropriated. Some of this may be connected to terrorist fundraising.
- **Cyber-enabled scams** e.g. using established 'social engineering' techniques to elicit personal or corporate information from individuals to then trick businesses into diverting or rerouting funds into criminally controlled bank accounts.

Read the latest UK government Advice on how to protect yourself and your business from fraud and cyber crime **here**.

Home Office

CASE STUDY | Stopping Face Masks Scams

- In March 2020, a Singaporean national was arrested for his alleged involvement in a business email impersonation scam in which a European pharmaceutical company was defrauded EUR 6.6 million (around SGD 10.2 million) through a purported sale of surgical face masks and hand sanitisers.
- After the company transferred the funds to a bank in Singapore, the items were not delivered, and the supplier became uncontactable.
- The Anti-Scam Centre (ASC), a new public-private partnership set up within the Singapore Police Force, worked with several Singapore-based banks, including Standard Chartered Bank, to freeze the necessary bank accounts. Through swift collaboration with the banks, the Police were able to recover SGD 6.4 million of the scammed assets.

[Source: Channel News Asia]

How is Standard Chartered Bank collaborating to mitigate the financial fraud and cyber threats?

- Participating in country-led Financial Information Sharing Partnerships to exchange intelligence with law enforcement agencies, such as the UK National Crime Agency (NCA) and peer bank institutions, to build collective understanding of the COVID-19-related Financial Crime threats.
- Actively engaging with the Cyber Defence Alliance (CDA) and National Cyber & Forensic Training Alliance (NCFTA) COVID-19 working groups to build understanding and exchange intelligence on the COVID-19 cyber-related threats.
- Collaborating internally across global teams to undertake investigations into our potential exposure to COVID-19 related financial crime, sharing operational and strategic intelligence on potential criminal threats across the bank to raise staff awareness and help to protect our clients and customers.

COVID-19 (Corona Virus) Financial Crime Risk Bulletin

April 2020

What might be indicative of suspicious COVID-19-related commercial or financial activity?

The indicators below should be considered in conjunction with all published guidance on fraud and financial crime 'red flags' They should also be evaluated in the context of the normal and expected activity of the client or customer, and other available information, to determine if the activity identified meets any reporting thresholds for 'suspicion':

- Cash intensive businesses, particularly service sector food and beverage companies or health and beauty establishments, operating in countries with COVID-19-related social restrictions, still depositing large amounts of cash through branches or ATMs, despite an expectation of limited to zero business activity. The cash could be the proceeds of drugs trafficking or human trafficking and modern slavery.
- COVID-19-related transactions for medical supplies or equipment between entities that do not appear to have clear or obvious lines of business relevant to COVID-19 issues, e.g. payments to real estate companies or general traders.
- Unusual requests from clients, customers or suppliers to change usual business or payment processes e.g. changing destination bank accounts for payments, or switching payment communication methods.
- Unusual withdrawals or diversion of funds in the accounts of businesses with a history of financial re-structuring or credit difficulties or facing enforcement proceedings. While this may be due to changing commercial circumstances caused by the pandemic, such businesses may be in a state of heightened vulnerability to fraud or money laundering activity from corrupt insiders or criminal groups.
- Accounts that have previously been dormant suddenly receiving funds connected to COVID-19 related items e.g. Personal Protective Equipment (PPE), hand sanitiser and other medical supplies or equipment.
- Unusual deposits into accounts connected to COVID-19 Charity or crowd funding. While there are large volumes of legitimate charity fundraising initiatives currently active, there are also a number of scams seeking to 'raise funds' for vaccines and medical equipment.
- New or unusual cryptocurrency transactions that may relate to COVID-19-related ransomware payments or potential 'fund raiser' crypto currency scams for vaccines e.g. 'Coronaviruscoin'
- Single accounts appearing to receive multiple payments from COVID-19-related government support and relief schemes with no reasonable explanation, especially where these are rapidly disbursed to multiple bank accounts and/or withdrawn in cash

CASE STUDY | Phishing with Intent

In April 2020, Google reported it was blocking more than 18 million phishing emails every day purporting to offer COVID-19 information, impersonating the World Health Organisation (WHO) advice or various international government financial aid and relief schemes.

A UK-US government issued **joint advisory note** listed common examples of phishing email subject lines as:

- 2020 Coronavirus Updates
- Coronavirus Updates
- 2019-nCov: New confirmed cases in your City
- 2019-nCov: Coronavirus outbreak in your city (Emergency).

[Sources: Google, BBC, NCSC]

[Source: Interpol]

STAY SAFE, STAY VIGILANT .

Law enforcement partners warn that criminal networks may be increasingly targeting remote workers, using inducements or threats against staff to obtain sensitive data. If you are concerned that you or a colleague may have been approached in this way, **you may wish to consider contacting the police to seek advice and support.**

Here for Good. Find out more about how Standard Chartered Bank collaborates with partners to protect and support our customers and clients from the impact of financial crime, on our public website here.