مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

وحدة المعلومات المالية
Financial Intelligence Unit

Dubai Financial Services Authority

ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

# TYPOLOGIES IN THE FINANCIAL SECTOR

Investigations and pro-active risk analysis of emerging risks likely to be prevalent across the financial sector in the United Arab Emirates (UAE), whilst taking into consideration the country's inherent financial crime risk, current COVID-19 pandemic impact, and business environment.

# Abstract

This Typology Report (the "Report") has been put together, as part of understanding the Money Laundering ("ML"), Terrorist Financing ("TF"), Sanctions, Fraud, Bribery and Corruption ("B&C") risks identified by the financial sector.

**Supervisory Authorities Sub-Committee and the Financial Intelligence Unit**
In the United Arab Emirates

"The Supervisory Authorities, chaired by the Central Bank of the UAE, the Financial Intelligence Unit (FIU) and the private sector have worked closely to address ML/TF-specific trends and typologies emerging from COVID-19 in the financial sector. Although these risks are still in the early stages of identification, the FIU along with supervisory authorities released this report to share COVID-19 related typologies and indicators to the private sector in order to remain abreast of emerging risks, and to mitigate them."

**H.E Khaled Mohamed Balama**
Chairman of NAMLCFTC

"The Executive Office on AML/CFT of the UAE have co-ordinated domestically with the FIU and supervisory authorities to assess the impact of COVID-19 on AML/CFT risks and systems."

**H.E Hamid Al Zaabi**
Director-General of the Executive Office AML/CFT of the UAE

# Introduction

The Supervisory Authorities Sub-Committee, the Financial Intelligence Unit in the UAE and the Executive Office for AML/CFT have jointly produced a typology report to address emerging risks in a timely fashion.

A pilot of financial institutions were selected to collaborate on an operational initiative that aims to share certain practices observed in the market amongst financial institutions and to engage actively with competent authorities when such typologies are identified.

## Outlining risks derived from the typologies identified by the financial sector that are **over and above** the risks outlined in the UAE's National Risk Assessment (NRA)

## Money Laundering (ML) and Terrorist Financing (TF) Risk

A proactive analysis of financial sector risk identified several issues likely to be prevalent across the whole financial sector, over and above those risks outlined in the UAE NRA.

It is important to note that a combination of these indicators may also raise ML and TF concerns from a modern slavery and human trafficking perspective.

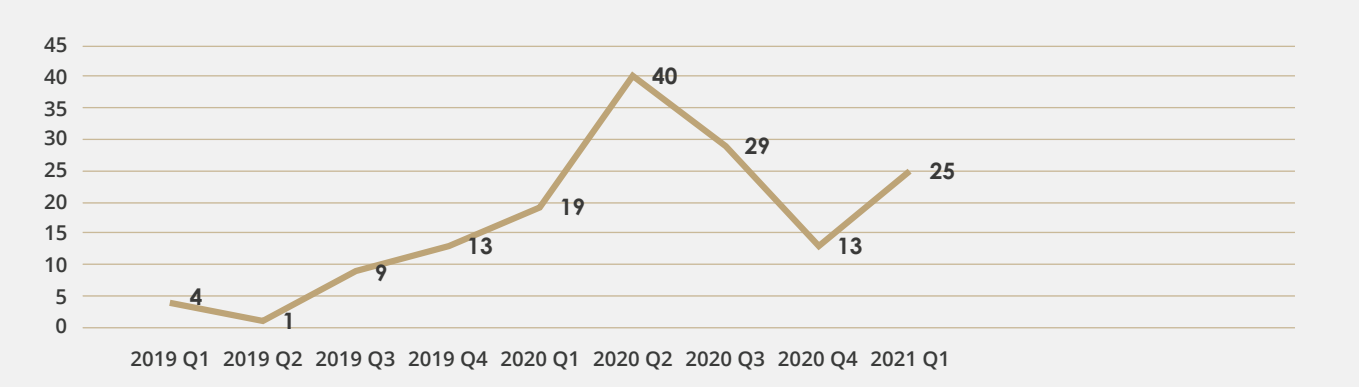
**Increased Use of Unlicensed Money Service Operators**

The use of unlicensed money service providers ("UMSO") for ML has increased during the COVID-19 pandemic. UMSOs do not move funds for each transaction but balance the books over a period, conducting a "money transfer without money movement". Although people will move funds legitimately through UMSOs for reasons of speed and convenience due to speed and convenience, the anonymity UMSOs offer means they are particularly appealing for financial criminals.

The following are some risk indicators, which could be common ML/TF techniques and could be used in combination to further obscure the true nature of the transaction, such as:

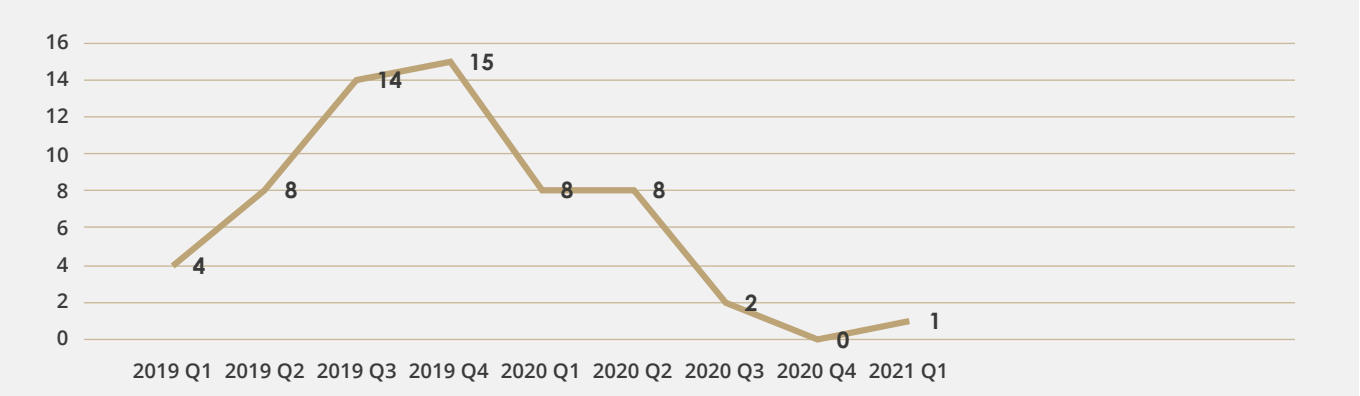
- General traders
- Transacting with incommensurate counterparties
- Receiving and sending funds rapidly
- Often zero daily balances
- Exceeding USD 100m turnover in the first year
- Large number of daily transactions
- Generic "payment details" descriptions
- Frequent payments to retail customers

## Trend analysis of one of the national banks in the UAE that illustrates the number of customers that utilise the underground banking / alternative remittance services (Hawala): Individuals




- There is a strong correlation between the increase in customers that utilise the Underground Banking / Alternative Remittance Services (Hawala): Individuals during the Covid-19 pandemic (in terms of period)
- High volume of internal transfers between accounts and cash activity which is not consistent with the profile of the customer
- Rapid movement of funds in the account that is not in line with the customer's business activity or profile
- Repeated small deposits from different counterparties in round amounts and fewer large transfers to single or multiple counterparties
- Funds are structured in a manner to avoid detection

## Trend analysis of one of Emirati bank in the UAE that illustrates the number of customers utilising the underground banking / alternative remittance services (Hawala) - Judicial persons




- The trend above illustrates a downward trend (lower number of customers that utilise the Underground Banking / Alternative Remittance Services (Hawala) - Judicial persons) during the Covid-19 pandemic
- Immediate withdrawals (through cheques and outward wire transfers) followed the crediting of funds rapidly
- Customers were unable to provide documentation and economic rationale for the underlying transactions

**Professional Money Laundering ("PML") Services**

The use of PML services is likely to increase during COVID; PMLs use a variety of money-laundering methods, including those that do not require the physical movement of cash or goods. Criminals who have previously relied on self-executed money laundering schemes may now be seeking the help of PMLs.

PMLs run several types of money laundering networks, including 1) Money Transport and Cash Controller Networks[1]; 2) Proxy Networks[2]; 3) Money Mule Networks; and 4) Digital Money and Virtual Currency Networks.[3]

The following are risk indicators, which could be common ML/FT techniques and could be used in combination to further obscure the true nature of the transaction, such as:

- Recent account opening by individuals / entities from high risk jurisdictions
- Minimal transactional activity for an extended period after account opening
- Test payments prior to "activation" of the account for illicit activity
- Rapid and significant increase in transactional activity
- Extensive use of cheques
- Matching credit and debit turnovers
- Counterparties in sectors which appear inconsistent with the stated business nature of the client

**E-Commerce Front Companies / Transaction Laundering**

Widespread lockdowns have resulted in a significant surge in e-commerce. Due to limited ability to move funds and goods during the pandemic, illicit actors are turning to e-commerce as a money laundering tool, which can be executed in two ways:

- **Front Companies** – fake digital storefronts that look like legitimate merchants, but are not in the business of selling the advertised goods; and
- **Pass-through Companies / Transaction Laundering** – illicit businesses using a legitimate merchant's platform to process illicit payments. This is referred to as "money laundering of the digital age", which is extremely difficult for financial institutions to detect.

  The following are some of the high risk indicators:

  **Transactional Activity**

  - Sudden sharp increase in e-commerce customer's turnover
  - The turnover is not consistent with the risk category assigned by the bank to the merchant

  **Customer's Website**

  - Unusual pricing of products in comparison to the expected or average market price
  - Spelling errors
  - Not user-friendly
  - Not updated frequently (this can be checked through archive.org)

  **Suspicious elements of the website**

  - The disclaimer "We only sell in bulk quantities"
  - Odd sizing scheme when selecting clothing items e.g. shirts

1 Criminals and OCGs that generate significant amounts of cash often use the services of cash controller networks that are capable of transferring vast sums of cash on their behalf. These international controller networks have the capacity to receive, hand over and transfer criminal proceeds, while charging a processing fee. Generally the structure of these networks consists of individuals who control, co-ordinate, collect and transmit illicit funds and who operate together to negotiate deals with the OCG.

2 Proxy networks are PMLs who supply a type of banking service to OCGs, generally with multi-layered transfers via bank accounts. These specialised services offer all of the advantages that come with moving funds globally via the legitimate financial sector. The main task of these proxy networks is to move client funds to the final, pre-determined destination and to obfuscate the trail of the financial flows.

3 PMLs also arrange schemes that allow criminals to cash out proceeds generated in virtual currency via online illicit markets (e.g. Dark Web drug-trafficking marketplaces). In many cases, payments for illicit drugs purchased online are transferred to e-wallets held in fiat currency or in virtual currency (e.g. Bitcoin). Afterwards, virtual currency is transferred through a complex chain of e-wallets, which may include the use of mixers and tumblers to further enhance the anonymity of the virtual currency transactions. Funds are then sent back to the e-wallet of the OCG, and subsequently transferred to bank cards and withdrawn in cash.

**Virtual Currencies ("VCs") for Money Laundering**

The use of VCs may be intensifying during the COVID-19 pandemic, as every criminal earning VC illegally ultimately looks for ways to covert third party proceeds into cash or other assets.

Whilst most Banks' AML policies do not allow for banking of VC exchanges, however, most Banks do bank some of the Third Party Payment Providers and payment gateways, which in turn may deal with VCs.

Most VC trades reportedly take place through Over-The-Counter ("OTC") brokers who facilitate trades between individual buyers and sellers who are not willing to transact on an open exchange; or through Peer-to-Peer ("P2P") platforms.

The following are high risk indicators:

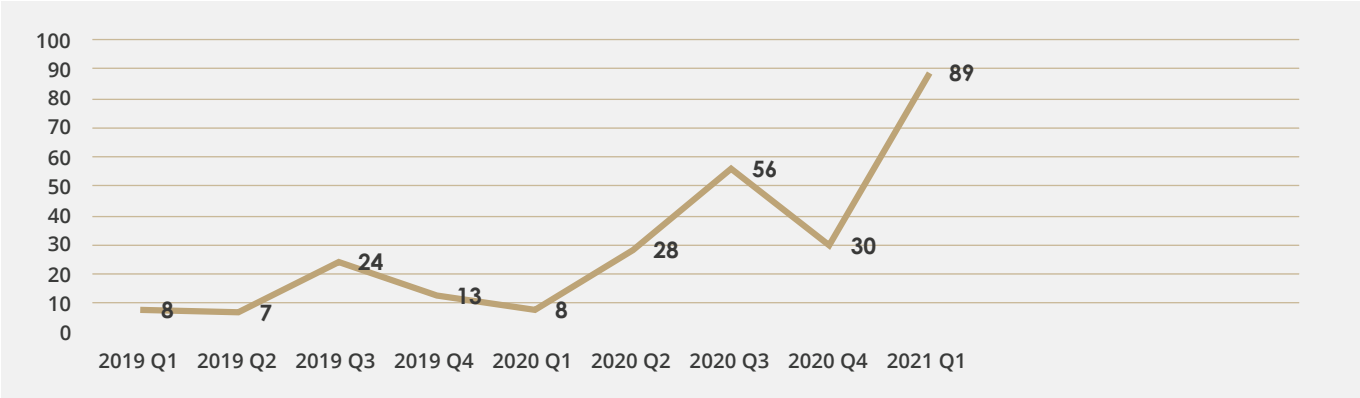
- One-off transactions
- Fewer high-value inbound payments and numerous low-value outbound transfers
- Transactions in multiple foreign currencies
- Business in IT, software or technology
- Return payments
- Relationships with sub-contracted industry intermediaries

**Money Mule Activity**

The number of "money mules" increased to launder ill-gotten funds, a result of widespread financial distress.

- Account activity indicates several structured cash amounts or cross-border remittances from unknown parties, which are immediately withdrawn / transferred, leaving nominal balances in the account
- The credits were mainly followed by immediate withdrawals through cash and / or mobile transfers
- In the majority of the cases reported to the FIU, it was observed that mule accounts were from low income individuals from African and Asian Nationalities

## Trend analysis of one of the national banks in the UAE that illustrates the number of customers that were suspiciously reported on money mule activity:




- The trend above suggests a strong correlation between COVID-19 pandemic peaks and an increased number of customers reported for suspicious money-mule transaction activity.

| | |
|---|---|
| **Shifts in Outflows (Values) to High Risk Jurisdictions** | Increased and unexplained cross-border fund flows to high risk jurisdictions during COVID-19 pandemic. |
| **COVID-19 Themed Fundraising** | Terrorist organisations seek to raise funds under the guise of COVID-19 related relief activities. |
| **Online Exploitation** | Exploit the need of impoverished or financially distressed communities to seek other revenue sources. |
| **Forced Labour** | Increased exploitation of vulnerable communities. |
| **Financial Crime Risks presented by Citizenship by Investment Schemes** | Citizenship by Investment ("CBI") schemes offered by countries located in the Caribbean region pose potential financial crime risks to the Financial Sectors in the UAE. Although CBI schemes may be pursued for legitimate purposes, in particular visa free access to the EU, the UK and other countries, CBI schemes pose corruption, sanction, money laundering and tax evasion risks. Typologies identified are as follows:<br>• Individuals seeking to hide the proceeds of corruption may choose to invest in a second passport in order to evade local authorities when moving funds<br><br>PEPS applying for CBI in the Caribbean region posing heightened financial crime risks include:<br>• Individuals exploiting shortcomings in the transparency and governance of some CBI schemes, including the use of government approved agents that may further increase FC risks<br>• Individuals seeking to gain tax residence in countries that operate CBI schemes with no personal income tax and that do not participate in the OECD's Global Common Reporting Standard |

## Fraud Risk

Based on our internal investigations and proactive risk analysis, the following fraud typologies were identified that are likely to be prevalent across the rest of the Financial Sector, given the current financial duress and volatile business environment.

**Corporate Fraud: Economic Distress and Susceptibility to Financial Crime**

Distressed companies may be tempted to widen their risk appetite to increase income, or reduce compliance, thus increasing their exposure to illicit counterparties. Some may also be susceptible to criminals offering money in return for use of their banking facilities. Businesses in the construction, cleaning services, wholesale, and consultancy sectors may warrant additional scrutiny, and can indicate money laundering or terrorist financing, when the activity is suspicious and / or does not appear to have a reasonable business or legal purpose.

The following are risk indicators which could be common money laundering / terrorist financing techniques and could be used in combination to further obscure the true nature of the transaction, such as:

- Negative news on a customer
- Companies changing company profile details to meet requirements for financial relief provided by governments
- Sudden influx of finance, through cash deposit
- Lack of transactions to known tax authorities
- Adding large number of beneficial owners in short space of time
- Initial low amount of cash deposits or inward bill payment followed by immediate small value outward transactions to newly added beneficial owners
- Account turnover exceeds estimate on account opening
- Rapid movement of funds, either withdrawn or transferred overseas
- Use of common / free domains instead of a listed work email address

**Corporate Fraud: Risks Presented by Domestic Trade & Related Parties**

The typology is defined by the abuse of domestic trading schemes with related party companies as further defined by a number of indicators that exhibit signs of the corporate fraud typology. These indicators include:

- No supporting documentation and difficulties in validating / corroborating the movement of goods and related transportation;
- Use of multiple connected / affiliated parties as goods suppliers to create complex business models;
- Customers that trade with general trading companies with no or limited physical presence;
- Complex ownership structures, often with a common management structure;
- High proportion of transactions conducted with the use of cheques, not in line with the expected account and business profile;
- High value trade partners that are local companies with no borrowing facilities with any other financial institution.

**Corporate Fraud Schemes**

The typology is defined by the different corporate fraud schemes, including:

- Double financing - where the same set of trade financing documents are presented to multiple banks, a commodity trader is engaging in double financing. Commodity traders using multiple banks in an end-to-end transaction may present high risks of fraud

| | |
|---|---|
| **Corporate Fraud Schemes** | • Two-way trading & documentation presentation – where a business entity that seeks financing to both export and import of the same commodity may be an indicator of a wholesale fraud risk. Two-way trading is not de facto risky, however, in instances where there is no valid business justification for two-way trading, it is perceived as high risk<br>• Unknown/Low Profile Counterparties - Companies engaged in commodity trading and those that carry out high value business with entities that have little established presence or low reputation could pose financial crime risks |
| **Corporate Fraud: Risks Presented by the Financial Accounts** | • Some of the high risk indicators used in combination and observed in Financial Accounts could be indicative of the attempt to obscure the true nature of the transaction, such as:<br>  • Rapid deterioration in financial performance<br>  • Incomplete or inaccurate accounts<br>  • Significant change in turnover and volume<br>  • Changes in auditors or the use of lower-tier auditors, relative to the size of the business<br>  • High net working capital relative to industry norms, rising faster than sales<br>  • High cash and high debt, frequent capital raising, persistent differences between cash flows and income / Earnings Before Interest, Taxes, Depreciation, and Amortisation<br>  • Suspicion that cash balances are not accurately reflected |
| **Corporate Fraud: Risks Presented in Trade Documents** | Some of the high risk indicators observed in Trade Documents are as follows:<br>• Invoices without company logos, or with incomplete addresses, suspicious contact details, vaguest descriptions of goods, round numbers, repeated amounts, strange invoice number patterns<br>• Bills of lading that look suspicious, e.g. as if they have been altered, or are not consistent with invoices<br>• Very complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good |
| **Government Stimulus Schemes or Aid Programmes** | Parties (individuals and entities) submitting false claims to qualify for relief facilities and or other government support during the relief period. |
| **Disaster and Investment Scams** | Fake fundraising campaigns, advance-fee scams, fraudster use deception to solicit donations, investment or other type of 'good cause' financial contribution. |
| **Product Scams** | Customers or counterparties selling counterfeit, unapproved or misbranded products to the bank's customer or to the general public. |
| **Impersonation Fraud** | Business email compromise or stolen personal information / data that seek to defraud the company, employees, customers or partners. This includes impersonated government officials, given the increasing number of schemes to support their citizens. |
| **Crypto-currency** | Typically connected with cybercrime (blackmail demanding ransom payments in crypto-currencies), Investment scams (ICO). |

## Bribery and Corruption ("B&C") Risk

Based on our internal investigations and proactive risk analysis, the following indicators, in combination, may raise money laundering concerns from a B&C perspective.

**On-boarding Indicators**

Some of the high risk indicators observed as part of the on-boarding process are as follows:

- Substantial wealth lacking satisfactory explanation, incommensurate with client turnover and not in line with the customer profile
- Reluctance to answer questions relating to sources of wealth
- Inaccurate information about the source of funds and / or the relationship with the counterparty
- Unusual questions of the financial institution's record-keeping or reporting requirements with the apparent intention of avoiding them
- Newly established companies having "Goods Wholesaler" in their title with no specific business line / customers
- Newly established LLC companies acting as fronts
- Old companies being purchased by new owners, however new owners having no information about the old companies operations and non-availability of companies bank statements or VAT returns, which seemingly appears to be acting as fronts
- Companies approaching for account opening where bank account has been closed by another bank
- Companies shareholders having no past business experience and are young individuals who have recently arrived in the UAE and seem to be acting as fronts

**Know-Your-Customer (KYC) Indicators**

Some risk indicators observed as part of the Account transaction and activity review, could be used in combination of other factors to further obscure the true nature of the transaction, such as:

- Refusal to honour requests to provide additional KYC documentation or to provide clarity on the source of funds
- Establishing company or trust, without adequate explanation
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner

**Transactions and Behavioral Indicators**

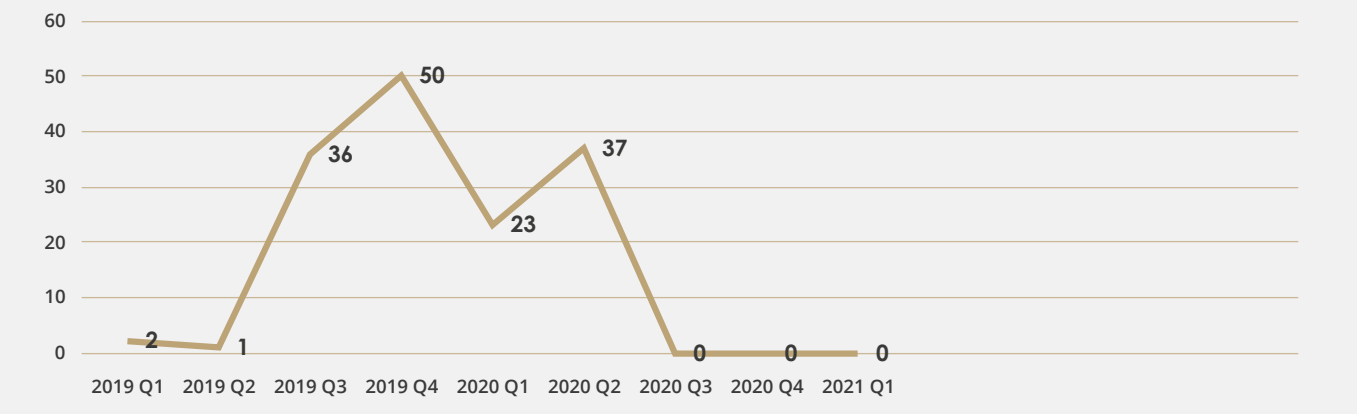
Some risk indicators observed as part of the Account transaction and activity review, could be used in combination of other factors to further obscure the true nature of the transaction, such as:

- Round-number payments, received from un-associated 3rd parties
- Large cash deposits, lacking adequate explanation
- Transactions to or from offshore corporate vehicles without transparent beneficial ownership
- Outward or inward wires from trusts, professional services firms, or unusual corporate vehicles, that lack adequate explanation
- Significant / unusual donations to charities or educational institutions
- Sudden spike in payments to family members, particularly if they're based in countries that rank highly on the secrecy index and / or to jurisdictions with weak AML control frameworks (to consider ratings on Basel AML Index)

**Transactions and Behavioral Indicators**

- Sudden spike in payments to accounts identified as private bank accounts based in secrecy jurisdictions and / or to jurisdictions with weak AML control frameworks (to consider ratings on Basel AML Index)
- Outward or inward wires from trusts, professional services firms or unusual corporate vehicles that lack adequate explanation
- Sudden spike in outflows of purchases of luxury items such as vintage cars or yachts, expensive art pieces, designer bags, or prime real estate in centers of luxury spending
- Calls made by the bank for transaction inquiries to customer's registered mobile numbers and the calls are answered by unknown persons
- On inquiry, customer seems unaware about high value credit received in their account
- Discrepancies in Company VAT returns and Company account turnover activity
- Receipt of funds from recognised or apparent Virtual Assets exchanges in small multiples potentially below the daily cash reporting threshold to avoid triggering system alerts
- Accounts are primarily funded with cash deposits in multiple locations across the UAE at the same time, which suggests that multiple parties conducted these deposits
- Cash deposits followed by cash withdrawals conducted mainly within one / a specific location
- Carrying out multiple ATM cash deposits in short succession (potentially below the daily cash reporting threshold) across various locations into a few selected banking accounts (i.e. concentration accounts)
- High volumes and large amounts of inflows, mainly through cash and remittances, which are immediately withdrawn or transferred out in large values to different Far East Asian jurisdictions such as China, Hong Kong, Taiwan, Singapore, Malaysia, Thailand, Indonesia, Vietnam and Philippines

## Trend analysis of one of the national banks in the UAE that illustrates the number of customers with large cash deposits / inward remittance followed by cross border outward wires:




- The trend above reflects the number of customers making large cash deposits during the period of the pandemic (e.g. upwards of December 2019, peaking in March 2020 and continues to date with return to office at social distance measures)
- Transactions do not appear to have a proper economic rationale as customers were not forthcoming with supporting documents
- Once opened, the account remains in a 'hibernated' state or dormant, often for multiple weeks and a sudden surge in activity through large value credits followed by immediate cross-border outward wires is observed

**Typologies observed from March 2019 – March 2021**

# Heightened External Fraud Threat on account of COVID-19

The outbreak of COVID-19 and its global spread has created significant challenges to society and risks for the economic outlook, although the severity of the economic impact continues to be evaluated.

As we continue to monitor and learn more about the spread of COVID-19 in our communities, we have recently observed heightened external fraud threat, especially with cyber criminals exploiting both traditional and digital channels, to remotely perpetrate cyber-enabled fraud attacks at scale in a rapidly evolving environment. The following types of fraud are most relevant in this context:

## 1. Social Engineering

We continue to see an increase in phishing and smishing attacks. Scammers are taking advantage of fears surrounding COVID-19. They set up websites to sell bogus products, and use fake emails, texts, and social media posts as a ploy to take money and get personal information from customers. They misrepresent organisations such as banks, government, the World Health Organisation or other health service providers. Websites ask for donations for victims promotingawareness, prevention tips and in some cases offering a 'cure' for the virus.

## 2. Online Fraud

COVID-19 has increased demand for online Grocery Shopping as consumers stock up on food and other essentials due to the outbreak. Customers who want to avoid the crowds are turning to the internet to shop. As more consumers try to avoid human contact, retailers are offering online shopping services. As such, fraudsters are also taking advantage of this online traffic to attack merchants to steal customer data or create websites to scam customers.

## 3. Brute Force attacks

The term 'brute force attack' refers to a type of fraud that involves a 'trial and error' approach to identifying a customer's personal credentials such credit card number, expiration date and card verification number. These attacks can also occur on account details such as a username and password so attacks specifically targeting credit card credentials are sometimes referred to as Bank Identification Number (BIN) attacks or credit master attacks. Typically, a fraudster will access a third party merchant payment page and use specialised software that will churn through various combinations of credit card numbers until a match is made. In this type of attack, the fraudster will know a victim's 6-digit BIN number and will attempt to guess the remaining digits as well as the expiration date and card verification code/value.

## 4. Credential Stuffing and Account Takeover (ATO)

When successful, credential stuffing attacks - in which troves of usernames and passwords are "stuffed" into bank login pages - allow fraudsters to access a victim's bank account. These attacks are becoming more widespread as criminals use stolen credentials to access accounts and leverage technology that enable them to bypass fraud controls, mimicking victims' profiles by fabricating browser or device identities, employing the same plugins, and altering geographic locations and time zones, especially as criminals have increasingly found it is easier to take over a new account than open a new one.

## 5. Application Fraud

While the emergence of COVID-19, we have seen a surge of customers applying for Loans, top-ups and credit cards to manage their financial requirements due to revenue losses on the personal and business fronts. We have also seen an increase in 1st and 3rd party fraud amongst the credit hungry population within our portfolio. "Red flag" activity that we have observed includes an increase in applications submitted with potentially-fraudulent KYC documents, including inflated income figures.

## 6. Trade Fraud

The COVID-19 virus is having a significant disruptive effect on commodity prices, business travel, and supply chain. Many factories around the world have closed down and sales have dropped significantly for certain businesses, as consumers stay and work from home. Foreign Exchange (FX) volatility has been significant, leading to material losses on some derivative contracts for some customers.

This is undoubtedly placing an unprecedented strain on several of our wholesale customers. In Q1 2020, we observed a significant increase in the number of high value investigations pertaining to allegations of wholesale fraud, where:

- Longstanding customer relationships find themselves under significant financial duress and may face insider

risk of resorting to manipulation of financial statements or falsified trade

- New and existing relationships controlled by elements of criminality who seek to exploit the current disruption by committing trade fraud through "pump and dump" strategies of maximising credit facilities and then skipping the country
- Existing relationships who may have been leveraging up over the recent years of financial incline through double financing and round tripping, are now exposed to an environment of new economic turmoil

The above hypothesis is most likely to potentially result in trade finance fraud consisting of over / under invoicing, double financing and ghost shipments. Furthermore, one cannot exclude the use of possible shell companies in Free Trade Zones, typically General Trading companies, that are de-facto undisclosed related parties and that can be used to facilitate illicit money flows and the typologies outlined above.

The suspension of trading for two (2) FTSE 100 UAE based companies in 2020, on allegations of fraud and material misstatement of financials through undisclosed borrowing, is also a concern. It is a concern; fraud occurs in large, listed companies. Questions around the effectiveness of corporate governance structures have rightly been raised and add to the overall environment of high risk indicators for corporate fraud and embezzlement in 2020.

## COVID-19 Outbreak: Risks of Charity / Disaster Fraud

### 1. Charitable Solicitations

Charity fraud is the act of using deception to get money from people who believe they are making donations to charities. Often a person or a group of people will make material representations that they are a charity or part of a charity and ask prospective donors for contributions to the non-existent charity.

### 2. Price Gouging / Profiteering

Price gouging is a term referring to when a seller increases the prices of goods, services or commodities to a level much higher than is considered reasonable or fair, and is considered exploitative, potentially to an unethical extent. Usually this event occurs after a demand or supply shock.

Tech Companies Take Action: Facebook, Amazon and eBay have taken steps to reduce potential exploitation by vendors of medical face masks, hand sanitizers and other products. Facebook banned adverts and commerce listings of medical facemasks, which do little for the public but are necessities for health practitioners caring for the ill. Meanwhile, Amazon and eBay took steps to stop price gouging on a range of products on their commerce platforms, including toilet paper.

### 3. Contractor / Vendor Fraud

Contractor and vendor fraud occurs when individuals pose as contractors or repairmen or financiers, but have no intention of actually repairing damage or completing the job. We have observed few occurrences of vendor fraud especially during a time when global attention is focused on the fight against the pandemic and the global effort to vaccinate populations and during the shortage of face masks, where fraudsters and organised crime syndicates attempted to exploit the situation by exploiting the shortages and disrupted supply chains.

### 4. COVID-19 Outbreak: Risks of Financial Misrepresentation and Trade Fraud

The following are the high risk sectors where the COVID-19 outbreak is having a severe impact, which is already leading to a rise in financial crime misrepresentation and trade fraud, due to a variety of reasons including financial distress and business challenges, such as those associated with the current economic downturn.

- Travel (particularly airlines and associated services)
- Tourism, hospitality and entertainment (hotels, travel agents, tour providers)
- Haulage, shipping and logistics
- Restaurants and other services
- Manufacturing companies that have supply chains dependent on where productions may be disputed by COVID-19

## Heightened Risk of Cyber-Attacks Amidst the COVID-19 Pandemic

Cyber risks have taken on greater prominence as reliance is placed on technology to assure operational continuity and companies and their employees shift towards remote working models to restrict the spread of the virus. This brings to the forefront the digital vulnerabilities such as phishing attacks, hacking, malware intrusions and fraud stemming from potential information breaches containing personally identifiable information.

Remote working models in a distributed work environment magnify the vulnerabilities of potential cyber-attacks. This is an important factor to address where documents containing confidential customer and/or financial information are shared between staff via a distributed work environment.

Organisations should prepare for possible business disruption and proactively assess their cyber hygiene practices followed by their remote workforce, enterprise-wide. To curtail any security incidences, organisations should consider the following effective cyber hygiene practices, which are not limited to:

- Ensure Virtual Private Network (VPNs) and other remote access systems are fully patched
- Enhance system monitoring to receive early detection and alerts of suspicious activity Implement multi-factor authentication (MFA)
- Ensure all devices have proper configured firewalls, as well as anti-malware and intrusion prevention software installed avoid clicking on links in unsolicited emails and be wary of email attachments
- Double-check any links by hovering over them to ensure you will not be redirected to a fraudulent website
- Review URL domain names for typos and/or missing characters x Restrict the sharing of personal or financial information in emails, and do not respond to email solicitations for such information
- Refer to trusted sources and legitimate, government websites for up-to-date, fact-based information about COVID-19