



Republic of Botswana

GUIDANCE NOTE FOR DETECTION OF COVID-19 RELATED CRIMES

FIA

FINANCIAL INTELLIGENCE
AGENCY



INTRODUCTION

Various governments across the globe implemented measures to contain the impact of COVID-19 on individuals and businesses. In most cases, government resources have been reprioritised towards responding to COVID-19 by implementing measures ranging from social assistance, financial support and tax relief initiatives, to enforce confinement measures and travel restrictions. In Botswana measures such as distribution of food baskets, wage support and subsidy schemes, tax relief measures and post corona economic stimulus package. It has been observed by many countries that while unintended, these measures provided new opportunities for criminals to generate and launder illicit proceeds.

The Financial Intelligence Agency (FIA) is issuing this advisory to alert Financial Institutions to fraud, corruption, and other predicate crimes for money laundering observed during the period of the COVID-19 pandemic. This advisory contains descriptions of the observed trends relating to fraud and associated red flag indicators. This paper is informed by information and reports shared by other countries, open-source research, information from suspicious transaction reports, and feedback from law enforcement partners. The indicators contained herein are likely to evolve as the crisis further develops.



COVID-19 RELATED CRIMES

Global law enforcement authorities have detected a wide range of COVID-19-related fraud and theft involving a variety of criminal actors. The following examples are a non-exhaustive list of this type of criminal activity.

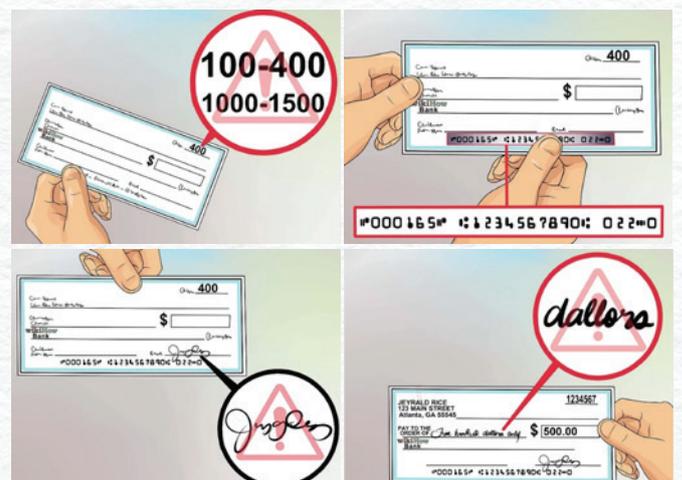
Corruption: Public officials suspected to have misallocated COVID-19 relief funds by misdirecting contracts to businesses that do not exist or have no reasonable business purpose, which ultimately benefit their own interests and/or financial gain. This typology includes government contracts for Personal Protective Equipment (PPE) and other healthcare supplies being unduly awarded to newly established businesses which ultimately benefit themselves or family members. Similarly, COVID-19 relief funds may have been inappropriately used to pay for items that have no benefit(s) to help stop the spread of COVID-19.



Abuse Of Public Procurement Processes: Emergency procurement of PPEs and other healthcare supplies created an opportunity for corrupt public officials to abuse their powers to circumvent laid down procurements processes for their personal gain. This led to award of procurement contracts to undeserving entities, overpriced supplies and delivery of substandard goods.



Fraudulent Cheques: Fraudsters send potential victims fraudulent cheques, instructing the recipients to call a number or verify information online in order to cash the fraudulent COVID-19 cheques. Victims are asked for personal or banking information under the guise that the information is needed to receive or speed up their COVID-19 relief payment. Fraudsters then use the information obtained to commit various crimes, such as identity theft and the unauthorized access of bank accounts.



Altered Cheques: Fraudsters deposit altered COVID-19 cheques, often via Automated Teller Machine (ATM). These altered cheques may modify the name of the payee, or leave the name blank, and the amount may be altered prior to deposit. There is reporting of cheques being chemically altered so the original payee is removed.

Counterfeit Cheques: Fraudsters deposit counterfeit COVID-19 cheques, often via ATM. Fraudsters have various methods to create a counterfeit cheque, including cheques reproduced from digital images of cheques issued by government agencies. However, such counterfeit cheques will often have irregularities involving the check number, paper, colouring, and/or font.

Theft: Such thefts can include requesting disbursement for an ineligible person; seeking another person's COVID-19 relief funds without the payee's knowledge and/or approval, or through coercive means; or using stolen Personally Identifiable Information (PII), including providing false bank account information to the Revenue Authorities to claim relief funds.



Phishing schemes using COVID-19 relief funds as a lure: Fraudsters perpetrate phishing schemes using emails, letters, phone calls, and text messages containing keywords such as "Corona Virus," "COVID-19," and "Stimulus," with the purpose of obtaining PII and account information, such as account numbers and passwords.

Inappropriate seizure of COVID-19 relief funds: A private company that may have control over a person's finances or serves as his or her representative payee seizes a person's funds, for wage garnishments or debt collection, and does not return the inappropriately seized payments.

Covid-19 relief loans – In an effort to support private businesses and stimulate the domestic economy, some governments guaranteed loans to tax compliant businesses. Some businesses which took up this form of support but diverted the money to fund other projects outside the country.

Wage subsidy fraud – some governments provided financial support to employees in sectors of the economy, who became technically unemployed on a temporary basis due to the impact of the COVID-19. Some companies created ghost employees to increase wage subsidy claims while directors/shareholders in private companies who are at the same time employed as government officials claimed the wage subsidy thereby double dipping from government coffers. Some employers did not pass on the wage subsidy to employees as per scheme requirements.



RED FLAG INDICATORS OF FINANCIAL CRIMES RELATED TO COVID-19 RELIEF FUNDS

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider all surrounding facts and circumstances to determine if a transaction is suspicious or indicative of potentially fraudulent activities related to COVID-19. In line with a risk-based approach to compliance, specified parties also are encouraged to perform additional inquiries and investigations where appropriate.

FIA has identified the financial red flag indicators described below to alert financial institutions to potential fraud, corruption, and thefts related to COVID-19 relief funds as well as to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such activities. Based upon each reporting entity's risk-tolerance level, exposure to risk, and in accordance with a risk-based approach, these red flags may result in the filing of a Suspicious Transaction Report (STR).

 An existing account receives, or an account holder makes, multiple COVID-19-related deposits for individuals other than the account holder(s), and the individuals named do not have a relationship with the account holder. This may be indicative of funnel account activities in which multiple payments are deposited or transferred into one account, which may be held by a fraudster or a money mule working for the fraudster.

 An existing account receives an excessive number of COVID-19 relief deposits related to a prepaid debit card linked to the same address (e.g., an account receiving more deposits than expected relative to the customer's profile and financial institution's customer due diligence).

 A customer opens a new account with a COVID-19 relief cheque, and the name of the potential account holder is different from that of the depositor or the payee.

 A COVID-19 relief deposited or transferred into dormant accounts with little or no prior activity.

 Rapid transfers of multiple relief payments into one account could indicate that bad actors are consolidating the payments. After the funds are consolidated, the funds may be quickly (a) withdrawn via large cash withdrawals or serial ATM withdrawals; (b) used to purchase convertible virtual currencies; (c) transferred out of the account via a money services business such as cryptocurrency exchangers and peer-to-peer mobile payment systems or wire transfers to other accounts; or (d) transferred onto prepaid debit or gift cards.

 An account receives several COVID-19 relief deposits and almost immediately thereafter (a) disburses funds for large purchases at merchants that offer cash back as an option, in amounts not typical of this type of merchant, or (b) has funds transferred onto prepaid debit or gift cards.

 Deposits of one or more relief cheques or electronic deposits made into an account held by (a) a business, or (b) a personal account of a business owner or employee and the account holder is not the payee/endorser. This may indicate that the business is using identifiers of its employees or customers to apply for their benefits for the purpose of inappropriately collecting the payments.

 An account holder attempts to deposit one or more cheques that appear to be issued for COVID-19 relief, but are fraudulent or counterfeit cheques. When questioned, the customer may disclose that he or she:

- was sent a partial payment, and needed to verify his or her PII or financial information before receiving the full payment; or
- received the check purportedly from a current or former employer with instructions that the cheque was the customer's "relief payment" and that he or she was to buy prepaid cards and send them to another individual.

 The same Internet Protocol (IP) address is used to transfer funds from an account which received COVID-19 relief funds, to several bank accounts or electronic wallets, especially if that IP address is associated with a business.

 An account receives (a) numerous deposits or electronic funds transfers (EFTs) that indicate the payments are linked to COVID-19 relief.

 An account with several COVID-19 relief deposits also receives numerous tax refunds for individuals other than the account holder(s). The names indicated on the COVID-19 relief deposits and tax returns may be the same but are not those of the account holder(s).

 Deposits of one or more COVID-19 relief cheques or electronic deposits are made into a nursing home or assisted living facility's business account and those payments have not been given to the resident. This may be an indication that the business is inappropriately withholding residents' relief funds.