NEW ORLEANS POLICE DEPARTMENT OPERATIONS MANUAL

CHAPTER: 41.38

TITLE: FINANCIAL FRAUD AND WHITE-COLLAR CRIME INVESTIGATIONS

EFFECTIVE: 12/22/2024
REVISED: NEW CHAPTER

PURPOSE

The purpose of this Chapter is to provide personnel of the New Orleans Police Department with protocol for accepting, recording and investigating economic crime offenses.

POLICY STATEMENT

1. NOPD is the primary investigatory agency for the investigation of complaints of financial fraud and white-collar crimes such as Louisiana Revised Statutes relating to Theft by Fraud; Residential Contractor Fraud; Access Device Fraud; Bank Fraud; Financial Elder Abuse; Identity Theft; On-line, Email and Telephone Scams; Skimming Devices; Counterfeit Currency; and Cryptocurrency Fraud.

2. The White-Collar Crimes Unit of the NOPD Investigative and Support Bureau has the primary responsibility to investigate large scale financial crimes, and to assist officers and detectives in their investigation of on-scene reported violations by providing advice and resources for the gathering of information and evidence relative to the crimes involved.

DEFINITIONS:

Definitions relevant to this Chapter include:

Access Device Fraud (RS 14:70.4) – Possession without authorization and with the intent to defraud, an access device or counterfeit access device issued to another person- defined as a person's social security number, driver's license number, birth date, mother's maiden name, checking account numbers, savings account numbers, personal identification numbers electronic identification numbers, digital signatures, or other means of account access that can be used to obtain anything of value.

Bank Fraud (RS 14:71.1) – The offender executes or attempts to execute, a scheme or artifice to defraud a financial institution or to obtain any of the monies, funds, credits, assets, securities, or other property owned by or under the custody or control of a financial institution by means of false or fraudulent pretenses, practices, transactions, representations or

promises.

Cryptocurrency – A digital currency exchanged through a computer network that is not reliant on any central authority, such as a government or bank to uphold or maintain it, available through a crypto ATM. Fraud can occur through an account takeover common with stolen phones, data breaches and malware.

Counterfeit Currency (RS 14:72) – The issuance, possession, selling, or otherwise transfer of a counterfeit or forged monetary instrument of the United States with the intent to defraud.

Financial Elder Abuse / Disabled Person (RS 14:67.21) – The wrongful or unauthorized taking, withholding, appropriation, or use of money, assets, or property of an eligible aged adult or disabled person. The trusted person with 'power of attorney', or the caretaker, must act with fiduciary responsibility to pay for care and benefit of the elderly or disabled person and cannot use the principle's funds to buy themselves things, sign over property through threats, or by taking advantage of altered mental capacity to secure financial fraud.

Fraud – An act of intentional deception designed to exploit a victim.

Identity Theft (RS 14:67.16) - The intentional use, possession, transfer, or attempted use, with fraudulent intent, by any person of any personal identifying information of another person to obtain, possess, or transfer, whether contemporaneously or not, credit, money, goods, services, or anything else of value without the authorization or consent of the other person.

Monetary Instrument Abuse / Counterfeit Currency (RS 14:72.2) – The offender makes, issues, possesses, sells, or otherwise transfers a counterfeit or forged monetary instrument with the intent to deceive.

NFC or Near Field Communication - a technology that allows devices like phones and smartwatches to exchange small bits of data with other devices and read NFC-equipped cards over relatively short distances. The technology behind NFC is very similar to radio-frequency identification (RFID) commonly used in the security cards and keychain fobs that you likely already use to get into your office or gym. In fact, NFC is an evolution of RFID that offers more advanced features and better security, but the two technologies still share a lot of things in common.

Online, Email and Telephone Scams (RS 14:67) – The offender contacts the victim through false pretenses to trick the victim into sending money, cryptocurrency, or divulging confidential information towards a financial or business advantage. Examples include the Business Email Compromise, the Romance Scam, the Sweepstakes Scam, the Officer Impersonation Scam, the Kidnapped or Injured Loved One Scam, and the Refund Scam.

Residential Contractor Fraud (RS 14:202.1) – Fraudulent conduct, practices, or representations by a person who has contracted or subcontracted to perform any home improvement or residential construction and fails to perform any work during a 45-day period of time or longer after receiving payment; uses any deception, false pretense or false promise to cause a person to enter into a contract; knowingly makes a material misrepresentation of fact in any application for a required permit.

RFID or Radio Frequency Identification - a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person.

Skimmers (RS 14:67.4) – The installation of an electronic device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card with the intent to defraud the authorized user, the issuer of the authorized user's payment card, or a merchant.

Theft by Fraud (RS 14:67) – The misappropriation or taking anything of value which belongs to another, either without the consent of the other to the misappropriation or taking, or by means of fraudulent conduct, practices, or representations.

Venue (CCrP Art. 611) – When an offender is charged with Unauthorized Use of an Access Card; Identity Theft; Access Device Fraud; Illegal Transmission of Monetary Funds; Bank Fraud; Forgery; and Monetary Instrument Abuse, the offense is deemed to have been committed either in the parish where the offense occurred or where the victim resides.

Wedge or wedge device - a tool used in fraudulent activities, particularly in manipulating contactless payment systems. It acts as a middleman between a legitimate card and the payment terminal, allowing attackers to intercept and alter the communication between them. This can enable unauthorized transactions without needing the cardholder's PIN.

White Collar Crimes Unit (WCCU) – The investigative unit within the NOPD Investigative and Support Bureau that is charged with investigating large scale financial crimes greater than $50,000, offenses where several individuals are acting in concert as a group to commit financial fraud crimes in concert, the victim is a financial institution such as a bank or large private institution. The WCCU also serves as the liaison between the United States Secret Service (USSS) and the rest of the NOPD to investigate federal financial crimes as deemed necessary. The WCCU also supports officers and detectives by providing knowledge to investigate on-scene violations involving financial crimes and to follow up on said crimes when necessary.

INITIAL ON-SCENE INVESTIGATING OFFICER RESPONSIBILITIES

1. Responding Officers receiving a call or complaint from an individual reporting that they have been the victim of a financial fraud (listed below) that is less than $50,000 in losses, shall document the criminal offense in an initial NOPD Incident Report. Those financial fraud crimes include:
    a.) Theft by Fraud;
    b.) Residential Contractor Fraud;
    c.) Access Device Fraud;
    d.) Bank Fraud;
    e.) Financial Elder Abuse;
    f.) Identity Theft;
    g.) On-line, Email and Telephone Scams;
    h.) Skimming Devices;
    i.) Counterfeit Currency; or
    j.) Cryptocurrency Fraud

2. Officers may work with District Investigative Unit (DIU) detectives as necessary for follow-up responsibilities to gain incident case closure.

3. The investigating officer and assisting detective may contact the White-Collar Crimes Unit for guidance and access to available resources in the gathering of information and evidence relative to the crimes involved. The WCCU can assist in:

    a.) determining the proper charges related to the items in the possession and actions of the suspect(s);

b.) lend resources such as equipment for detection of counterfeit notes and credit cards;
c.) refer financial crimes contacts such as bank investigators, and
d.) contact Secret Service Agents when necessary.

4. All notifications to the WCCU should be conducted via email to whitecollarcrimes@nola.gov unless the reported crime involves any of the following:
    a. Crypto currency;
    b. Business email compromises;
    c. A suspect has been detained; or
    d. Any cases involving over $50,000.

    Cases involving any of the above listed factors require notification to WCCU by phone or through the Orleans Parish Communications District (Dispatch).

5. All cases involving Crypto currency require immediate notification by phone or through dispatch to the WCCU.

6. Email notifications to the WCCU should not be considered a transfer of investigative responsibilities to the WCCU without approval of the WCCU supervisor.

DETERMINING JURISDICTION OF OFFENSE

7. Under the Louisiana Code of Criminal Procedure Article 611, if the offender is charged with Identity Theft, Access Device Fraud, Illegal Transmission of Monetary Funds, Bank Fraud, Forgery or Monetary Instrument Abuse (these charges will cover most types of fraud), the offense is deemed to have been comitted either in the parish where the offense occurred or where the victim resides.

8. If the victim resides in Orleans Parish and the offense occurred in another parish or the offense occurred in Orleans Parish and the victim resides in another parish, the initial responsing officer from NOPD shall take the report, whether the actual fraudulent transactions occurred in Orleans Parish or not. Officers shall not advise the victim to call another agency to file a report.

CONTRACTOR FRAUD

9. The most common method of contractor fraud is the contractor not having the appropriate license or not completing the work after payment is received. Work must begin within 45 days of payment unless otherwise stated in the signed and dated contract.

10. A Commercial License is required on all commercial projects of $50,000 or more (also acts as Home Improvement License). A Residential License is required for residential projects exceeding $75,000. A Home Improvement License is required if the contract exceeds $7,500 and does not exceed $75,000.

11. When investigating Contractor Fraud, officers should obtain a copy of the contract if one exists, copies of any checks or other means of payments, and all pertinent information on the contractor such as name, license number and contact information.

12. An incident report shall be prepared under RS 14:202.1 Residential Contractor Fraud. The White Collar Crimes unit shall be notified on all incidents involving conractor fraud via email at whitecollarcrimes@nola.gov.

ACCESS DEVICE FRAUD

13. Offenses involving an access device (check) include the cashing of fraudulently altered or 'washed' checks where the payee and the amount is changed to gain unauthorized financial advantage. The offense also includes the selling, possessing, or giving of the checks or other information to someone other than the original payee.

14. Offenders who obtain money from a bank by depositing or cashing a stolen or altered check are to be charged with acess device fraud.

15. All stolen, forged or altered checks shall be collected by the investigating officer as evidence.

16. An incident report shall be prepared under RS 14:71.1 - Bank Fraud. The White Collar Crimes unit shall be notified on all incidents involving acess device fraud.

FINANCIAL ELDER ABUSE / DISABLED PERSON

17. Investigating officers shall identify if the designated caretaker misused the elderly, aged or disabled principle's funds for personal gain (trips, meals, gas, personal bills). The victim's funds may only be used for the care and benefit of the prinicipal (bills, food, clothing).

18. The investigating officer shall identify if the offender has been granted one of the various types of Power of Attorney, or a court order and obtain Power of Attorney. The signed and dated Power of Attorney or court order shall be attached to the investigative report.

19. There are five recognized types of Power of Attorney:

- **Limited or Special Power of Attorney**: grants an agent the authority to act on behalf of the principal for a specific purpose or time period.
- **General Power of Attorney**: grants an agent the authority to act on behalf of the principal for a broad range of matters, such as financial, legal, or business affairs.
- **Durable Power of Attorney**: grants an agent the authority to act on behalf of the principal even if the principal becomes incapacitated or unable to make decisions.
- **Springing Power of Attorney**: grants an agent the authority to act on behalf of the principal only if the principal becomes incapacitated or meets a certain condition.
- **Medical Power of Attorney**: grants an agent the authority to make health care decisions for the principal if the principal is unable to do so.

20. Execution formalities require the POA to be signed by the principal. In Louisiana, signatures must occur in the presence of two witnesses. Additionally, the document must be notarized. The witnesses and notary attest that the principal signed voluntarily and is competent. These formalities are necessary for the POA to be valid under Louisiana law. Powers of Attorney in Louisiana must:
    a. Written Document - A POA must be documented in writing to be legally binding.
    b. Signature -Both the principal and the agent must sign the POA.
    c. Notarization And Witnesses -Most POAs require notarization and witnesses. This ensures authenticity and prevents fraud.
    d. Specific Language -Louisiana mandates precise legal language to clearly define the scope and authority granted in the POA.

21. Investigating officers should also be aware of theft incidents when the caretaker may

force or coerce the elderly principle to change their will or sign over property by taking advantage of altered mental capacity (dementia, alzheimer's).

22. An incident report shall be prepared under RS 14:67.21 Theft of the Assets of an Aged Person or Disabled Person. The White Collar Crimes unit shall be notified on all incidents involving financial elder abuse /disabled person.

IDENTITY THEFT

23. Procedures for the investigation of incidents under RS 14:67.16 Identity Theft are outlined in **NOPD Chapter 41.39 - Identity Theft.**

ONLINE, EMAIL, AND TELEPHONE SCAMS

24. A cybercrime fraudulent offense occurs when the "scammer" uses Email to trick someone into sending money or divulging confidential information. Scammers use phishing or malware to get access to an individual or company's critical and confidential information to exploit or defraud for financial gain.

25. Scammers may utilize the telephone to misrepresent themselves and deceive victims into sending money, gift cards, or cryptocurrency under false pretenses.

26. Reported complaints for these types are to be considered as a Theft as they are committed through the use of fraudulent conduct, practices, or representations. Officers are to obtain all contact information for the scammer, how money was sent, and any documentation indicating the transfer of funds.

An incident report shall be prepared under RS 14:67 Theft by Fraud. The White Collar Crimes unit shall be notified on all incidents involving online, email and telephone scams

SKIMMERS

27. Skimmers are devices illegally installed on ATMs, point-of-sale (POS) terminals, or fuel pumps to capture credit/debit data or record cardholders' PINs. The equipment is installed internally, over a card reader, or over a keypad, and may also have a hidden camera.

28. Handheld devices (AKA: Wedges) are generally used at restaurants and other locations where the victim's card is given to an employee to scan. Some devices can also clone RFID and NFC cards. Data can be retrieved by the suspect via Bluetooth or removing the device.

29. If a device is located, officers should **limit physical contact** with the device as it is possible to obtain latent prints and DNA. Officers should also establish the chain of custody if this evidence is removed by an employee and contact the WCCU.

An incident report shall be prepared under RS 14:67.4 Anti-Skimming Devices. The White Collar Crimes unit shall be notified on all incidents involving skimming devices.

COUNTERFEIT CURRENCY

30. Officers conducting an investigation into the <u>intentional</u> possession or transfer of counterfeit currency shall confiscate the bills and place them into evidence. If there are security cameras at the location where the counterfeit currency was used, obtain a copy of the recorded exchange for evidence.

31. An incident report shall be prepared under RS 14:72.2 Monetary Instrument Abuse (Forgery). The White Collar Crimes unit shall be notified on all incidents involving counterfeit currency.

CRYPTO-CURRENCY INVESTIGATIONS

32. Fraud investigations may also involve the use or misappropriation of crypto-currency, as a medium of exchange transferred through a computer network. Victims may be instructed by scammers to withdraw money from their bank, access a crypto ATM, and then deposit funds to a reception point set up by the scammer.

33. Crypto can also be stolen from a victim through a fraudulent account takeover, common with stolen phones, data breaches and malware.

34. Fraudsters prefer crypto because it is believed harder to trace. The White Collar Crimes unit has the ability to trace crypto transactions. A timely notificaion increases the chances of rcovering funds through seizure.

35. Officers investigating a transfer or fraud involving crypto-currency shall obtain the following information:

    - The “public key” used to receive crypto from another person
    - The type and amount of crypto taken
    - The date/time it was transferred
    - The user name for the exchange, and
    - If an ATM was used, the location and receipt obtained

36. An incident report shall be prepared under RS 14:67 by Fraud.The White Collar Crimes unit shall be notified on all incidents involving crypto-currency in a fraud investigation.