316.1 ECONOMIC CRIMES / IDENTITY THEFT INVESTIGATIONS

I. PURPOSE: The purpose of this Standard Operating Procedure is to provide personnel of the Tampa Police with protocol for accepting, recording and investigating economic crime offenses.

II. SCOPE: This Standard Operating Procedure shall apply to all personnel assigned to investigate economic crime offenses.

III. DISCUSSION: Economic crimes, specifically identity thefts, are the fastest growing crimes in the United States, affecting financial institutions as well as innocent persons. Identity theft is a tool used by terrorists and others attempting to evade the law. The best way to approach any economic crime is to follow the money trail. By doing so you can generally ascertain the jurisdiction where the illegal act occurred and who the actual victims are. Ultimately, the victim is determined by whoever suffers the actual or potential loss. However, it must be kept in mind that although an individual may not suffer a financial loss they may still be a victim of identity theft. Therefore, the Tampa Police Department shall take the necessary measures to record criminal complaints, assist victims contacting other relevant investigative and consumer protection agencies, as well as work with federal, state and local enforcement agencies to identify and apprehend violators.

IV. DEFINITIONS:

A. Credit Card Check Fraud, and Identity Theft Form (TPD Form 883): A form provided to a credit card, check fraud, or identity theft complainant by the investigating officer or community service officer (CSO). The form contains instructions for a complainant who is interested in prosecuting the suspect in a fraudulent use of a credit card, check fraud, or identity theft case.

B. Check Kiting: Opening accounts at two or more financial institutions and using the "flat time" of available funds to create fraudulent balances.

C. Counterfeit: The manufacture of, or arranging to manufacture, a payment instrument without the permission of the financial institution, account holder, or organization whose name, routing or account number appears on the payment instrument, or the manufacture of any payment instrument with a fictitious name, routing or account number.

D. Counterfeit Credit Card: Any credit card which is fictitious, altered, forged, any facsimile or false representation, depiction, component of a credit card, or any stolen credit card, obtained as a part of a scheme to defraud or otherwise unlawfully obtained and which may or may not be embossed with account information or a company logo.

E. Credit Card: Any instrument or device, whether known as a credit card, credit plate, bank service card, check guarantee card, electronic benefits transfer card

(EBT), debit card, or any other instrument, issued by a financial institution for the use of the cardholder in obtaining money, goods, services or anything of value on credit or for use in an automated banking device to obtain any of the services provided through the device.

F. Elderly Person: (F.S. §825.101) A person 60 years of age or older who is suffering from the infirmities of aging as manifested by advanced age, organic brain damage or other physical, mental or emotional dysfunction, to the extent that the person's ability to provide for their own care or protection is impaired.

G. Payment Instrument: A check, draft, money order, traveler's check or other instrument for payment of money, whether or not negotiable.

H. Skimmer or Wedge: A device used to copy credit card numbers typically used at hotels, restaurants or car rental agencies. The device captures a credit card number after it passes through the device. Devices hold between 20 – 100 credit card numbers. **If a subject is found in possession of a skimmer or wedge, immediately notify the Economic Crimes Unit.**

I. Trade Secret: The whole or any portion or phase of any formula, pattern, device, combination of devices, or compilation of information which is for use, or is used, in the operation of a business and which provides the business an advantage or an opportunity to obtain an advantage over those who do not know it or use it. Examples include: Any scientific, technical, or commercial information including any design, process, procedure, list of suppliers, list of customers, business code or improvement thereof.

J. United States Treasury Checks: Any payment instrument issued by the United States Treasury Department.

V. COMMONLY COMMITTED OFFENSES:

A. Advanced Fee Scheme: (F.S.§817.034) The deceiving a victim into parting with their monies by convincing them that they will receive a substantial financial benefit in return for providing some modest payment to be made in advance.

B. Check Fraud: (F.S. §832.05) Checks that are stolen, altered, forged, or counterfeit, written on a closed account, or that have had payment stopped that are uttered, cashed or deposited resulting in the theft of money, merchandise or services.

C. Counterfeit Payment Instruments: (F.S.§831.28) It is unlawful for any person to have in their possession a counterfeit payment instrument or to counterfeit a payment instrument with the intent to defraud a financial institution, account holder, any person or organization. These include forged checks, counterfeit bills, deeds, money orders, traveler's checks, and credit/debit cards.

D. Depositing Worthless Item with Intent to Defraud: (F.S.§832.05[3]) Depositing counterfeit, stolen or other worthless checks for the purpose of fraudulently increasing the dollar amount posted to the account to which the individual then removes the monies before the financial institution discovers the checks are fraudulent.

E. Driver's License (Making or Possession of Material to Make): (F.S.§831.29) It is unlawful for any person to make or have materials or instruments intending to make counterfeit driver's license or identification cards.

F. Elderly Exploitation: (F.S.§825.103) Knowingly, by deception or intimidation, obtaining or using, or endeavoring to obtain or use an elderly person's funds or assets with intent to temporarily or permanently deprive that person of the use, benefit or possession of those assets by a person who: (a) stands in a position of trust and confidence with the elderly person; (b) has a business relationship with the elderly person; or (c) exploits an elderly person who lacks capacity to consent.

G. Embezzlement: (F.S.§812.014) Although there is no Florida State Statute that specifically pertains to embezzlement it is defined as the following: embezzlement relates directly to the theft statutes where a business has suffered a substantial financial loss through a scheme to defraud involving a current or former employee who was placed in a position of financial trust.

H. Financial Scams and Cons: (F.S. §812.014 or F.S.§817.034) Commonly referred to as "Bank Examiner" scam, "Pigeon Drop" scam, "Canadian Lottery" scam, "Spanish Lottery" scam and "Nigerian Fraud" scam.

I. Forgery: (F.S.§831.01) Whoever falsely makes (counterfeits), alters, forges an official public record, document or payment instrument, with intent to injure or to defraud.

J. Forgery of a Credit Card: (F.S.§817.60[6]) Any person who: with intent to defraud a purported issuer or a person or organization providing money, goods, services, or anything of value; of any other person; falsely makes, embosses, or alters in any manner a credit card or utters such a credit card or who, with intent to defraud, has a counterfeit credit card or any invoice, voucher, sales draft, or other representation or manifestation of a counterfeit credit card in his/her possession, custody or control.

K. Fraudulent Use of Credit Card: (F.S. §817.61) The use of credit cards, ATM cards or debit cards and/or ATM, credit or debit account numbers, that are stolen, altered, forged, counterfeit or obtained through fraud, resulting in the theft of money, merchandise or services.

L. Identity Theft (Criminal Use of Personal Identification Information): (F.S. §817.568) Any person who willfully and without authorization fraudulently uses or possesses,

with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual's consent.

M. Scheme to Defraud: (F.S.§817.034) (Also known as the Florida Communications Fraud Act). A systematic, ongoing course of conduct with intent to defraud one or more persons, or with intent to obtain something of value from one or more persons by false or fraudulent pretenses, representations, promises, or willful misrepresentations of a future act. These offenses include embezzlement, advanced fee schemes, financial scams/cons, financial elderly exploitation, check kiting, trade secret violations and computer-related financial crimes.

N. Trade Secret Violations: (F.S.§812.081) Any person who, with intent to deprive or withhold from the owner thereof the control of a trade secret or with intent to appropriate to his/her own use or the use of another, steals an article representing a trade secret, or without authority makes a copy.

O. Uttering a Forged Instrument: (F.S.§831.02 or 831.09) Knowingly passing and/or presenting of an official document or payment instrument which is counterfeit, having been altered or having a signature that has been forged, in the attempt or actual receipt of money, merchandise or services.

VI. RESPONSIBILITY / ROUTING:

The Tampa Police Department and other local and federal government agencies jointly and concurrently investigate many economic crimes.

A. Tampa Police Department's Economic Crimes Unit investigates the following offenses:

1. Identity Theft;

2. Schemes to Defraud (except those originating via mail or Internet):

   a. Embezzlement – Where a business suffers loss in excess of $5,000.00 from a suspect in a position of financial trust where the loss is due to credit card fraud, check fraud, or wire transfers;

   b. Advanced Fee Schemes; and/or

   c. Financial Scams and Cons;

3. Forgery/Uttering Forged Instrument;

4. Check Fraud;

5. Deposit Fraud;

6. Credit Card Fraud / Forgery;
7. Elderly (Financial) Exploitation;

8. Trade Secret Violations;

9. Counterfeit Currency; and

10. Possession of materials to Manufacture Fake Driver's License / Identification Cards.

B. The United States Postal Inspector's Office is responsible for investigating offenses involving stolen, forged or counterfeit postal money orders and mail theft. That agency also investigates schemes and scams originating through the U.S. Mail.

C. The United States Secret Service investigates offenses involving stolen or forged U.S. Treasury checks as well as counterfeit currency.

D. Fraud originating via the Internet: Since this type of fraud normally originates from outside of the United States and/or outside of the state of Florida, the victims of these types of offenses should be referred to the FBI's web site: www.ic3.gov: This type of fraud includes but is not limited to: Canadian Lottery Scam, Jamaican Lottery Scam, the Nigerian Check Fraud Scam,Business Email Compromises, Romance Scams, Identity Theft, Fraudulent use of Credit Card cases, or any other cases where the charges or accounts were opened online or the fraud occurred over the Internet to include money transfer applications.

E. Worthless Checks: This department does not handle complaints of worthless checks. Both misdemeanor and felony worthless check cases will be referred to the "Worthless Checks Section" of the Hillsborough County State Attorney's Office: 700 E. Twiggs Street, Suite 711 (7th Floor), telephone number (813) 272-5336.

F. Stop Payment and Closed Accounts: All check cases involving Stop Payment and Account Closed shall be investigated by this department after intent to defraud has been established. If there is doubt as to the intent initiate a report and refer the case to the Economic Crimes Unit.

G. Employee Theft: Cases involving employee theft involving cash will be referred to the appropriate District Latent Investigative Squad for investigation. Embezzlement cases where a business has suffered a loss of at least $5000.00, from the unauthorized use of a credit card, fraudulent checks, or a wire transfer, and where the suspect was in a **position of financial trust (i.e. business manager, bookkeeper, chief financial officer)**, shall be referred to the Economic Crimes Unit.

H. Burglary / Theft Offenses: In those cases where identity, checks, or credit cards are stolen and no leads exist, the cases should be inactivated. If the owner of the property determines that someone used any of those items within a 48-hour period the cases should be referred to the District Latent Investigative Squad for

investigation. If identity, checks, or credit cards are used after the initial 48-hour period, the cases should be referred to the Economic Crimes Unit for latent investigation. This includes where property is loaned by the victim to someone else and fraudulent activity occurs, whether the fraudulent activity is in person or over a payment application.

VII. PROCEDURES:

All sworn police personnel and community service officers are authorized to take reports on any economic crime. The on-scene district unit and district community service officers will primarily originate and collect all evidence pertaining to economic crimes. **REMEMBER TO OBTAIN SWORN STATEMENTS.**

Many times a suspect will leave some form of identification at the scene of an offense. Generally, it will be stolen, altered and / or counterfeit. Do not assume the identification is accurate enough to positively identify the suspect. Do not make an arrest or place a pick-up for a suspect based solely on identification left at the scene. Officers should obtain a sworn statement from the teller or clerk who conducted the transaction to verify how they identified the subject.

A. Identity Theft: Identity theft is punishable under federal law when any person knowingly transfers or uses without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a felony under applicable state or local law. [18 U.S.C. 1028(a)(7)].

Identity theft is punishable under F.S.§817.568. Any person who willfully and without authorization fraudulently uses or possesses with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual's consent commits a felony.

A victim may not normally know exactly where their identity was assumed. Per F.S.§817.568(16), a person is entitled to make an Identity Theft report where they reside, regardless of where it occurred. **However, when in doubt take a report.**

1. The victim must present documentation showing that their personal information was compromised.

2. Fully record information concerning criminal acts that may have been committed illegally using another's personal identity as covered by state and federal law.

3. Classify as identity theft fraudulent acts committed against an individual when there is evidence that the following types of unauthorized activities have taken place in the name of the victim:

    a. Credit card charges, debit cards, ATM;

b. Credit card checks written against the victim's account;
c. Credit card accounts opened or account addresses changed;

d. Establishment of a line of credit at a store or obtaining a loan at a financial institution;

e. Goods or services purchased in the victim's name;

f. Gaining access to secure areas; and/or

g. Used in the commission of computer fraud.

4. Obtain or verify the correct identifying information of the victim to include the date of birth, social security number, driver's license number, other photo identification, current and most recent addresses, email address, and telephone numbers.

5. Document the nature of the fraud or other crime committed in the victim's name.

6. Determine what types of personal identifying information may have been used to commit the crimes (i.e., social security number, driver's license number, birth certificate, phone numbers, email addresses, and credit card numbers), the state of issuance and whether any of the identifying information have been lost, stolen or potentially misappropriated.

7. Document any information concerning where the crime took place to include the address, the financial institutions or related companies involved, and the residence or whereabouts of the victim at the time of these events.

8. Determine whether the victim has knowledge or belief that a specific person or persons have used his or her identity to commit fraud or other crimes.

9. Determine whether the victim is willing to assist in the prosecution of suspects identified in the crime.

10. Determine if the victim has filed a report of the crime with other law enforcement agencies and whether such agency provided a report number.

11. If an entity other than the Tampa Police Department would be better suited to investigate the incident, document in the report what manner was used to refer the case to the other entity.

12. Refer all identity theft reports to the Economic Crimes Unit. If it appears that the identity theft may have national security implications, immediately notify the Criminal Intelligence Bureau and appropriate federal agencies.

B. Counterfeit Currency: The Tampa Police Department and the United States Secret Service investigate offenses related to counterfeit currency. Since there is concurrent jurisdiction, the decision to proceed with state or federal charges will be made by members of both agencies conducting the joint investigation.

1. When an officer encounters a person in possession of or uttering counterfeit currency with criminal intent they should notify the on-call Secret Service agent at (813) 228-2636.

2. Should the suspect, knowingly, be in possession of 10 or more counterfeit bills he should be charged with possessing counterfeit bills under F.S.§831.08 regardless of whether the suspect attempted to pass any of the bills.

3. Should the suspect, knowingly possess a counterfeit bill and attempt to pass that bill he should be charged with uttering a forged bill under F.S.§831.09 regardless of the number of bills in that subject's possession.

4. It is **not** a criminal offense for a subject to **unknowingly** possess counterfeit currency. However, F.S.§831.20 **mandates** all law enforcement officers to seize any counterfeit currency or counterfeit making material that comes to their knowledge. This administrative statute should be utilized when an officer comes in contact with a subject who unwittingly possesses counterfeit currency.

   Regardless of whether an arrest is made or not the officer shall seize the counterfeit bills, unless taken by the Secret Service agent, and place the bills in a clear plastic envelope before entering it into evidence. The officer shall initiate a report and obtain a written statement from all parties involved.

C. Other Economic Crimes: These include, but are not limited to: Identity Theft, Credit Card Fraud, Uttering Forged Instruments, Fraud, Embezzlement, and similar crimes.

1. In offenses concerning forged documents, the first arriving officer will detain the suspect and determine the kind of document involved in the forgery. The officer shall at all times protect the document from contamination. It should be noted that whether a transaction is completed or not, the presentation of a forged document constitutes the offense of Uttering a Forged Instrument and should be investigated as such.

2. In all cases of Forgery, the report taker will require the following documentation from the victim's financial institution:

   a. Affidavit of Fraud; or

b. Affidavit of Forged Signature; or

c. A Questionnaire of Fraudulent Use of a Credit / Debit Card; and

d. A copy of the victim's bank summary showing the losses, and location of the charges.

3. The report taker will research Tampa Police Department records for the owner or payee to determine if the document has been reported lost or stolen and determine if a police report has already been made.

4. If the report taker is unable to determine that the check and/or credit card has been lost or stolen, a copy of the documentation and identification, front and back, will be made and a report will be completed to document the circumstances. Place the original checks and/or credit cards in a plastic envelope, photocopy (after placing evidence in plastic) all items to include the FRONT and BACK and place it in the Evidence Control Section as evidence. The report will be referred to the Economic Crimes Unit.

5. Original evidence is the best evidence. The report taker should attempt to obtain any and all original documents that were stolen/forged As well as receipts for any purchase. All documents provided to law enforcement should be copied and attached to the report. All photographs uploaded into evidence.com should also be attached to the report by the originating officer.

6. Determine if there is surveillance video and/or photos available. If so, collect a physical copy, place into the property room as evidence, and notate in the report the witness that provided the video to law enforcement.

   a. If video is unable to be downloaded, request the video be copied and ready for law enforcement to pick up, and notate in the report that video is available.

   b. If the video is captured on bodycam, please notate in the police report. **Obtaining a copy of the video on bodycam is only considered a copy, and the original video from the store is still to be collected.**

7. Many times a suspect will leave some form of identification at the scene of an incident. Generally, it will be stolen, altered and /or counterfeit. Do not assume the identification is accurate enough to positively identify the suspect. In short, do not make an arrest or place a pick-up for a suspect based solely on identification left at the scene.

8. If investigating a financial crime where a personal computer or laptop computer is present and which may contain related evidence, do not touch it

and do not allow the suspect access to it. The suspect may have safeguards in place that could erase or delete important evidence data.

a. If the computer is OFF LEAVE IT OFF. Do not turn the computer on for any reason. Unplug the computer by pulling the power cord out of the back of the computer, not at the wall. Place the computer into the Evidence Control Section as evidence.

b. If the computer is ON DO NOT OPERATE THE COMPUTER. Do not attempt to confirm the computer contains evidence. Do not shut down the computer in a normal fashion. Unplug the computer by pulling the power cord out of the back of the computer, not at the wall.

c. Photograph the computer before touching it, including all wire connections and the monitor screen.

d. If the computer is a part of a network, contact the Economic Crimes Unit supervisor.

e. Place tape over all drive slots.

f. Label connectors and cable ends to facilitate re-assembly for forensic examination.

g. Keep equipment away from magnets and radio transmitters (such as in the trunk of a police vehicle).

D. Credit Card, Check Fraud, and Identity Theft Form (TPD 883): If the investigation determines there is probable cause to believe a crime was committed and the suspect is not known, but there are investigative leads, then the following procedure using the Credit Card, Check Fraud, and Identity Theft Form (TPD Form 883) will be utilized:

1. The investigating officer or Community Service Officer (CSO) will originate a police report. The investigative officer or Community Service Officer (CSO) will attempt to obtain all locations, to include the addresses, dates, and times for the fraudulent transaction(s). If there is more than one transaction, the victim will need to obtain the listed information for each additional transaction. A separate report will need to be originated for each location that fraudulent activity occurred.

2. In these cases, the General Offense Report will reflect the issuance of the Credit Card Check Fraud, and Identity Theft Form on the last line of the "case

summary" section by the officer including: "Credit Card, Check Fraud, and Identity Theft Form issued."

3. In those cases that the investigating officer has doubts as to the referral of the case, the officer should issue the Credit Card,Check Fraud, and Identity Theft Form to the complainant.
4. The police report will be referred to the Economic Crimes Unit.

5. The investigating officer will fill in the required information on the Credit Card, Check Fraud Form, and Identity Theft (TPD form 883). This includes indicating the offense, the complainant's information, date, complainant's address, and offense number. The officer will then provide the complainant the Credit Card, Check Fraud, and Identity Theft Form.

6. When issuing the form, officers are **NOT** to advise the complainant that a detective will contact them. The victim **MUST** comply with the instructions indicated at the bottom of the form and respond to the district office within ten (10) days.

VIII. ASSISTING VICTIMS:

A. Personnel taking reports of identity theft and other economic crimes should take those steps reasonably possible to assist victims in resolving their problems. This includes providing victims with the following suggestions where appropriate.

1. Provide the victim with the Tampa Police Department's "Victim Information Pamphlet" for guidance. The pamphlet provides the victim with information about what to do and about whom to call if they are a victim of identity theft.

2. Suggest the victim contact the Federal Trade Commission (FTC) at 1-877-IDTHEFT (438-4338) or at www.consumer.gov/idtheft. The FTC acts as the nation's clearinghouse for information related to identity crimes. The agency provides assistance from trained counselors in resolving credit-related problems. The FTC also provides a comprehensive guidance for victims of identity theft titled, "When Bad Things Happen to Your Good Name." The guide provides concrete steps of what to do when a person is a victim of identity theft.

3. Have the victim complete the Federal Trade Commission's sample affidavit. Obtain a copy of the complete affidavit. If the affidavit is notarized, it can be introduced to a grand jury in lieu of a victim having to appear. It can also be used as part of a victim's impact statement in later court proceedings.

4. Have victims cancel each credit/debit card. Request new cards and new account numbers.

5. Contact the fraud departments of the three major credit reporting agencies and ask that they put a fraud alert on the account. Be sure the fraud departments add an alert to contact the victim before opening new accounts in the victim's name.

   a. Equifax 1-800-525-6285 (or) 1-800-685-5000

   b. Experian 1-888-397-3742 (or) 1-888-EXPERIAN

   c. Trans Union 1-800-680-7289 (or) 1-877-553-7803

6. If bank accounts are involved, report the loss to each financial institution. Suggest the victim cancel all existing accounts and open new account numbers. Suggest the victim place stop payments on all outstanding checks.

7. If a driver's license is involved, contact the state motor vehicle department. If the driver's license agency uses that social security number, request a new driver's license number. Also check with the Social Security Administration to determine the accuracy and integrity of the account.

B. Often persons arrested will use the identity of another to conceal their true identity. Should a victim learn they have a Florida Criminal History due to another person using their identity an officer should provide the following assistance:

1. If the victim has not made a previous police report, take a report of identity theft.

2. Request that the victim initiate a compromised identity claim through the Florida Department of Law Enforcement (FDLE). This service is only for individuals who believe they are victims and/or have had their personal identification information stolen or misused in the past. To initiate a claim, the victim must complete a **Compromised Identity Review Claim Form**, which includes a fingerprint card. The victim may contact FDLE by calling 1-850-410-8109 or by going to www.fdle.state.fl.us/CompId.

   The victim must have his or her fingerprints taken directly on the claim form by a law enforcement agency. To ensure the integrity of the fingerprints, the law enforcement agency will then route the form to FDLE at the address provided. FDLE will only accept claim forms that are submitted by a law enforcement agency and in an official agency envelope. The victim will have to contact the law enforcement agency of their choosing to make arrangements to be fingerprinted.

   Upon receipt of the Compromised Identity Review Claim Form, FDLE

will compare the fingerprints of the person who was previously arrested, to the victim's fingerprints. Once these prints reveal that the victim was not the person arrested, FDLE will provide the victim with a **Compromised Identity Certificate**. FDLE will work with the law enforcement agency who has ownership of the criminal record/fingerprint file in an attempt to clear the charges listed under the victim's identity. FDLE will send the victim a letter advising them of their results.

Supersedes SOP 318, dated 4/22.