


FLORIDA HIGHWAY PATROL POLICY MANUAL

	SUBJECT IDENTITY CRIMES	POLICY NUMBER 22.16
		ISSUE DATE 04/01/10
		REVISION DATE 04/22/13
		TOTAL PAGES 7

22.16.01 PURPOSE

To establish procedures for investigating and handling the reporting of identity theft that may come to the attention of members of the Florida Highway Patrol.

22.16.02 POLICY

Identity crime is the fastest growing and most serious economic crime in the United States. The Florida Highway Patrol shall take the following measures to respond to identity crime:

- A. Record criminal complaints;
- B. Provide victims with copies of reports as required by federal law;
- C. Work with other federal, state, and local law enforcement and reporting agencies as well as financial institutions to solve identity crime cases;
- D. Seek opportunities to increase community awareness and prevention of identity crimes; and
- E. Provide identity crime training to members.

22.16.03 DEFINITIONS

- A. **IDENTITY CRIME** - The fraudulent use of another person's identifying information (such as credit cards, social security numbers or driver license numbers) with the intent to facilitate other criminal activities or to obtain credit, goods, or services without the victim's consent. No financial loss is necessary in order to have an identity crime case.
- B. **IDENTITY THEFT REPORT** - A police report that contains specific details of an identity crime is considered an identity theft report under Section 605B of the Fair Credit Reporting Act (FCRA).
- C. **IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT OF 1998 (FEDERAL)** - Identity Crime 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 any applicable state or local law.”

- D. **FAIR AND ACCURATE CREDIT TRANSACTION ACT (FACT ACT OR FACTA) OF 2003 (FEDERAL)** - Establishes requirements for consumer reporting agencies, creditors, and others to help remedy damages resulting from identity crimes. The FACT Act requires local law enforcement agencies to provide police reports to victims of identity theft. The FACT Act entitles consumers to obtain free credit reports once a year from each of the three reporting agencies.
- E. **IDENTITY THEFT PENALTY ENHANCEMENT ACT OF 2004 (FEDERAL)** - Amends Federal criminal code to establish penalties for a new crime: “aggravated identity theft”.

22.16.04 RESPONSIBILITIES

The Bureau of Criminal Investigations and Intelligence will investigate cases involving criminal use of personal identification, typically a Florida Driver License (D.L.) or Identification Card (I.D.), which meet the Agency’s Statewide Investigative Strategy when they are reported to or are identified by a member of the Division of Florida Highway Patrol or Department of Highway Safety and Motor Vehicles.

Typically, such cases are reported to and investigated by the appropriate law enforcement agency within a local jurisdiction, however the Division and BCII will work closely with federal, state and local law enforcement to arrest perpetrators of identity related crimes.

22.16.05 PROCEDURES

- A. **CRIMINAL USE OF PERSONAL IDENTIFICATION: INVESTIGATIVE GUIDELINES**
 - 1. Florida law provides that in a case involving criminal use of personal information that the initial report may be taken by the agency where the victim resides or where an element of the crime occurred. In the event a member is notified of the criminal use of personal identification, the member shall determine if the victim resides in or an element of the crime occurred in the state of Florida. If so, the member should complete the appropriate incident report and notify the Bureau of Criminal Investigations and Intelligence. If the victim does not reside in the state of Florida and if no elements of the crime occurred within the state, the victim should be directed to make an initial report to the appropriate local law enforcement agency.
 - 2. Pursuant to 817.568 (17), F.S., prosecution of criminal use of personal identification must be commenced within three years after the offense occurred. Prosecution may however, be commenced within one year after discovery of the offense, or by a person who has legal duty to represent the aggrieved party and who is not a party to the offense, if such prosecution is commenced within five years after the violation occurred.

3. Once the determination has been made that FHP will investigate a specific criminal use of personal identification case, the member completing the initial report shall ensure the following steps have been taken by the victim and note such in the initial incident report.
 - a. Have the victim complete the Identity Crime Incident Form, which can be obtained from the Federal Trade Commission (FTC) website at www.ftc.gov or contact can be made by telephone at 1-877-IDTHEFT.
 - b. Refer victim to the Attorney General's Office website at www.myfloridalegal.com/identitytheft for the purpose of completing the steps outlined in the "Florida Criminal Use of Personal Identification Victim Kit".
 - c. Advise the victim to begin gathering documents (bank and credit card statements, letters from creditors or collection agencies, etc.). Obtain authorization from the victim under "The Fair Credit Reporting Act" to obtain transaction records from their creditors without a subpoena.
 - d. Advise the victim to obtain consumer credit reports by contacting the fraud department of the three major credit reporting agencies:
 - (1) Equifax 1-800-525-6285
 - (2) Experian 1-888-397-3742
 - (3) Trans Union 1-800-680-7289
 - e. Explain to the victim the potential consequences of being a criminal use of personal identification victim.
 - f. Advise the victim of the Office of Attorney General/Statewide Prosecutor's Victim Advocacy Program.
4. The following guidelines should be considered by members while investigating criminal use of personal identifications:
 - a. Attempt to identify other associated victims/incidents (i.e., Fraud-Net, InSite, Consumer Sentinel (more information available at: www.ftc.gov/sentinel), local agency contacts, etc.).
 - b. Use traditional investigative techniques (i.e., tracking devices, mail covers, surveillances, trash pulls, telephone tolls, forensic analyses, etc.).
 - c. Make use of spreadsheets for the purpose of building account/victim databases.
 - d. Ask financial institutions for all information related to known addresses of potential fraudulent users.

- e. Ask financial institutions for all information related to known person identifying information.
- f. Look for common themes in locations where fraudulent information was used (e.g., cooperating merchant).
- g. Look for the source of the victim's identification compromise.
- h. Contact financial institution security departments; ask them what information is available and follow up with a subpoena.
- i. Contact merchant security departments.
- j. Obtain available information from postal inspectors reference P.O. Boxes, associated applications and forwarding instructions.
- k. Contact the Secret Service E-Information Network at www.einformation.usss.gov.
- l. All actions, progress and updates shall be documented in the Department's Criminal Information System Case Tracking program.

B. COMPLETING THE IDENTITY CRIME REPORT

An identity crime report entitles an identity crime victim to certain important protections that will help the victim eliminate fraudulent debt and restore their credit to pre-crime status. Identity crime reports should be completed by members (or the first member that has contact with the victim), in person with the victim, and in the jurisdiction in which the victim is a resident. Recording all relevant information and data in such reports is essential to further investigation. Therefore, members and/or supervisors should:

1. Obtain or verify identifying information of the victim including date of birth, social security number, driver license number, other photo identification, current and prior addresses, telephone numbers and email addresses.
2. Document the nature of the identity crime committed in the victim's name (i.e. when and how the crime was discovered, documents or information used in the crime, the manner in which the victim's identifying information was obtained, the financial institutions or related companies involved, etc.)
3. Determine what types of personal identifying information may have been used (i.e. social security number, driver license number, birth certificate, credit card numbers, etc.) and whether any of these have been lost, stolen, or potentially misappropriated.
4. Determine whether the victim authorized anyone to use his or her name or personal information.

5. Determine whether the victim has knowledge or belief that specific person(s) have used his or her identity to commit fraud or other crimes. If so, obtain information about the suspected person(s).
6. Determine whether the victim is willing to assist in the prosecution of the suspects identified in the crime.
7. Determine if the victim has filed a report of the crime with other law enforcement agencies and whether such agencies provided the victim with a report number.
8. Determine if the victim has additional documentation to support his or her claim or facilitate the investigation.
9. Provide the victim a copy of the completed identity crime report or the report number.
10. Forward the report through the chain of command to appropriate investigative officers and immediately to intelligence agencies (Fusion Centers, ICE, JTTF, etc.) and federal agencies if it appears to have national security implications. To avoid investigating a fraudulent identity crime complaint, local law enforcement agencies should conduct due diligence in their completion of identity crime reports. Otherwise, unless and until it develops that the complaint is fraudulent; identity crime complaints should be aggressively and fully investigated.

C. ASSISTING THE VICTIM AFTER THE IDENTITY CRIME REPORT IS COMPLETE

Members taking identity crime reports should take steps reasonably possible to help victims return to their pre-crime status. This includes providing victims with the following suggestions where appropriate:

1. Briefly describe the process that occurs after an identity crime report is completed (for example, the identity crime report will be assigned to an investigative officer, that officer will review the report and contact the victim with any follow-up questions or to conduct a detailed interview with the victim, the investigative officer will begin to gather evidence, etc.)
2. Provide the victim with contact information for a point of contact for his or her case.
3. Inform the victim of other available resources to help with recovery.

D. INVESTIGATING IDENTITY CRIME (BCII)

When tasked with the investigation of identity crime, BCII members should consider the following:

1. Interview of the victim:

- a. Review the identity crime report and conduct any follow-up inquiry of the victim for clarification or expansion of information.
 - b. Ask the victim to obtain a free credit report at www.ftc.gov/freereports, identify any fraudulent accounts on his or her credit report, and contact creditors to close those fraudulent accounts.
 - c. Ask the victim if he or she knows any addresses associated with any of the fraudulent accounts. This may help determine the jurisdiction where the suspect lives.
 - d. Ask the victim to provide a list of the creditors/merchants where the suspect has opened accounts in the victim's name.
 - e. Ask the victim if he or she has been a victim of theft (breaking and entering, larceny, auto theft, etc.) where their personal information may have been compromised or if the victim knows where his/her identity may have been compromised.
 - f. Suggest that the victim keep a log of his or her contacts with creditors/collection agencies to include the times and dates of the contact and purpose of the call.
 - g. Recommend the victim maintain contact with the agency where the report was filed and provide information obtained from credit checks related to additional crimes to that agency.
2. Contact the creditors/merchants/banks that have the fraudulent accounts:
- a. Determine how the accounts were opened.
 - (1) If the account was opened through the internet, determine if there is an IP address available.
 - (2) If the account was opened over the telephone, determine if the financial institution captured the telephone number that was used to open the account.
 - (3) If the account was opened in person, identify the witness who opened the account for the suspect or the witness who conducted the transaction.
 - b. Request relevant information from the involved financial institutions (e.g. customer record, signature card, transaction history, application, any videos or photos, etc.).
 - c. Obtain statements from witnesses regarding the transaction and the suspect.

3. Gather additional information.
 - a. Contact other involved or potentially involved law enforcement agencies for collaboration to avoid duplication. These include any state and/or local law enforcement agency with which the victim has filed a crime report or where there is an indication that the identity crime took place.
 - b. Contact the Federal Trade Commission (FTC) Consumer Sentinel Law Enforcement Network and search the database for investigative leads.
 - c. Search the FTC Clearinghouse for other reported complaints that may be related to the case and contact other agencies in the area to determine if there have been similar crimes reported and possibly connected.
 - d. Determine the extent of compromise to the victim's identity.
 - (1) Determine motive.
 - (2) Conduct trash pulls, surveillance, photo line-ups, interview, computer forensics.
 - (3) Run a criminal history and background check on the suspect, once a suspect is identified.
 - e. Use available databases to locate additional information or to tie the suspect to the victim.
 - f. Obtain search warrants (financial and residential), telephone records, and handwriting samples from the suspect.
 - g. If an IP address was obtained and used in the investigation, get a court order for the subscriber information.
4. Utilize investigative tools available on the Internet. For example:
 - a. www.einformation.usss.gov
 - b. www.ftc.gov
 - c. www.idsafety.org
 - d. www.gethuman.com
 - e. www.search.org/programs/hightech/isp
 - f. www.onguardonline.gov
 - g. www accurint.com
 - h. www.atxp.com
 - i. www.nationalanapa.com/index.html
 - j. www.blackbookonline.info/