CITY OF ANDERSON POLICE DEPARTMENT
Anderson, South Carolina

DIRECTIVE TYPE General Order	EFFECTIVE DATE January 29, 2010	NUMBER 1609
SUBJECT Identity Theft	REVISED January 28, 2010	
REFERENCE SCLEA 19.9	AMENDS/SUPERSEDES All Others	
DISTRIBUTION All Personnel	RE-EVALUATION DATE Annual	NO. PAGES 6

A. Purpose

The purpose of this policy is to provide law enforcement agencies with protocols for completing identity crime reports, investigating identity crimes, and preparing cases for identity crime prosecution.

B. Policy

Identity crime is the fastest growing and most serious economic crime in the United States. Although identity crime presents unique challenges, law enforcement agencies have an ethical and professional obligation to assist identity crime victims and bring criminals to justice. This law enforcement agency shall take the following measures to respond to identity crime:

1) record criminal complaints;
2) provide victims with necessary information to help restore their pre-crime status;
3) provide victims with copies of reports as required by federal law;
4) work with other federal, state, and local law enforcement and reporting agencies as well as financial institutions to solve identity crime cases;
5) seek opportunities to increase community awareness and prevention of identity crimes; and
6) provide identity crime training to officers.

C. Procedures

1. Completing Identity Crime Report (SCLEA 19.9 A-B)

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 police personnel (or the first officer 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, officers and/or supervisors should:

a. Obtain or verify identifying information of the victim including: date of birth, social security number, driver's license number, other photo identification, current and prior addresses, telephone numbers, and e-mail addresses.

b. 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.)

c. Determine what types of personal identifying information may have been used (i.e. social security number, driver's license number, birth certificate, credit card numbers, etc.) and whether any of these have been lost, stolen, or potentially misappropriated.

d. Determine whether the victim authorized anyone to use his or her name or personal information.

i. 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).

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

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

iv. Determine if the victim has any additional documentation to support his or her claim or facilitate the investigation.

v. Provide the victim a copy of the completed identity crime report or the report number.

vi. 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.

2. Assisting the Victim After the Identity Crime Report is Completed (SCLEA 19.9 C)

Officers 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:

a. 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.)

b. Provide the victim with contact information for a point of contact for his or her case. If possible, the point of contact should be the officer who completed the identity crime report or the assigned investigative officer. Advise the victim that he or she should allow 10 days before checking on the status of the investigation.

c. Provide the victim with IACP/Bank of America Victim's Toolkit (*Get Back Your Good Name*). If the toolkit is not immediately available provide the victim with the checklist in Addendum A.

d. Inform the victim of other available resources to help with recovery.

3. Investigating Identity Crime

Investigation of identity crime shall include, but not be limited to, the following actions where appropriate:

a. Interview the victim:

1. Review the identity crime report and conduct any follow-up inquiry of the victim for clarification or expansion of information.

2. 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.

3. 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.

4. Ask the victim to provide a list of the creditors/merchants where the suspect has opened accounts in the victim's name.

5. Ask the victim if he or she has been a victim of theft (breaking & entering, larceny, auto theft, etc.) where their personal information may have been compromised or if the victim knows where his or her identity may have been compromised.

6. 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.

7. 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.

b. Contact the creditors/merchants/banks that have the fraudulent accounts:

1. Determine how the accounts were opened. If the account was opened through the internet, is there an IP address available? If the account was opened over telephone, did the financial institution capture the telephone number which was used to open the account? If the account was opened in person, identify the witness who opened the account for the suspect or the witness who conducted the transaction.

2. Request relevant information from the involved financial institutions (e.g. customer record, signature card, transaction history, application, any videos or photos, etc.)

3. Obtain statements from witnesses regarding the transaction and the suspect.

c. Gather additional information: (SCLEA 19.9 D)

1. Contact other involved or potentially involved law enforcement agencies for collaboration to avoid duplication. These include any state and/or local enforcement agency with which the victim has filed a crime report or where there is an indication that the identity crime took place.

2. Contact the Federal Trade Commission (FTC) Consumer Sentinel law enforcement network and search the database for investigative leads.[2]

3. 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.

4. Determine the extent of compromise to the victim's identity.

5. Determine motive.
6. Conduct trash pulls, surveillance, photo lineups, interviews, computer forensics.
7. Run a criminal history and background check on the suspect, once a suspect is identified.

8. Use available databases to locate additional information or to tie the suspect to the victim.

9. Obtain search warrants (financial and residential), telephone records, and handwriting samples from the suspect.

10. If an IP address was obtained and used in the investigation, get a court order for the subscriber information.

d. Utilize investigative tools available on the internet. For example,

1. www.einformation.usss.gov
2. www.ftc.gov
3. www.idsafety.org
4. www.gethuman.com
5. www.rocic.com/links.htm
6. www.search.org/programs/hightech/isp
7. www.onguardonline.gov
8. www.accurint.com
9. www.atxp.com
10. www.nationalnanpa.com/index.html
11. www.blackbookonline.info/

By order of:

Martin D. Brown, Chief of Police

1-29-2010
Date

ADDENDUM A

☐ Advise the victim to keep a log of all conversations related to the crime and keep all correspondences related to the crime. This can be used as part of the victim impact statement during any subsequent court proceeding.

☐ Give the victim an Identity Crime Recovery Toolkit (www.idsafety.org) and advise them to visit www.idsafety.org for additional victim-related identity crime information.

☐ Advise the victim to cancel any fraudulent of compromised accounts. The victim must immediately close and dispute any unauthorized accounts whether those are credit card or charge accounts. The Federal Trade Commission (FTC) developed an "ID Theft Affidavit" that is accepted by many banks, creditors, other businesses and the credit bureaus. Direct the victim to www.consumer.gov/idtheft/ for a copy.

☐ Advise the victim to place a fraud alert on his or her credit report. The victim should contact one of the three credit bureaus to report the crime and place a fraud alert on his or her credit report: Equifax (800) 525-6285, www.equifax.com; Experian (888) 397-3742, www.experian.com; or TransUnion (800) 680-7289, www.transunion.com. Explain to the victim that once he or she places a fraud alert, he or she is entitled to free copies of his or her credit report.

☐ Advise the victim to visit the FTC's website and complete the FTC consumer complaint form at www.consumer.gov/idtheft/. Explain that the FTC is responsible for receiving and processing complaints from people who believe they may be victims of identity crime. The FTC provides informational materials to people impacted by identity crime and refers complaints to appropriate entities, including the major credit reporting agencies and law enforcement. Advise the victim to contact the FTC's Identity Theft Hotline at 1-877-IDTHEFT (1-877-438-4338) to receive telephone counseling from specially trained personnel to help them resolve credit-related problems that may result from the misuse of their identities. If the crime involves regular mail services, recommend that the victim contact the U.S. Postal Inspection Service at:
https://postalinspectors.uspis.gov/forms/MailFraudComplaint.aspx