A. Purpose

The purpose of this policy is to provide employees with protocols for accepting, recording and investigating the crime of identity theft.

B. Policy

Identity theft is one of the fastest growing and most serious economic crimes in the United States for both financial institutions and persons whose identifying information has been illegally used. Also a tool that terrorist and those who are attempting to evade the law can use to their advantage. Therefore, this agency shall take those measures necessary to record criminal complaints, assist victims in contacting other relevant investigative and consumer protection agencies, and work with other federal, state and local law enforcement and reporting agencies to identify perpetrators.

C. Definitions

Identity Theft: Identity theft is the wrongful use of another person’s identifying information - such credit card, social security or driver’s license numbers – to commit financial or other crimes. Identity theft is generally a means for committing other offenses such as fraudulently obtaining financial credit or loans, among other crimes.

D. Procedure

1. Legal Prohibitions
a. 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 any applicable state or local law. [18 U.S.C. 1028(a)(7)]

b. Identity theft is punishable under state law (S.C. Code 16-13-510) which states:

c. It is unlawful for a person to commit the offense of financial identity fraud.

d. A person is guilty of financial identity fraud when he, without the authorization or permission of another person and with the intent of unlawfully appropriating the financial resources of that person to his own use or the use of a third party:

(1) obtains or records identifying information which would assist in accessing the financial records of the other person; or

(2) accesses or attempts to access the financial resources of the other person through the use of identifying information as defined in subsection c.

(3) Identifying information includes, but is not limited to:

a) social security numbers;
b) driver’s license numbers;
c) checking account numbers;
d) savings account numbers;
e) credit card numbers;
f) debit card numbers;
g) personal identification numbers;
h) electronic identification numbers;
i) digital signatures; or
j) other numbers or information which may be used to access a person’s financial resource.
(4) A person who violates the provisions of this section is guilty of a felony and, upon conviction, must be fined in the discretion of the court or imprisoned not more than ten years, or both. The court may order restitution to the victim pursuant to the provisions of Section 17-25-322.

2. Taking Crime Reports (CALEA 42.2.8.a)

All sworn police personnel are authorized to take crime reports on identity theft. Recording all relevant information and data in such reports is essential to further investigation. Therefore, officers and / or supervisors should:

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

b. 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 victim’s name.

1) Credit card charges, debit cards, ATM cards.
2) Credit card checks written against their account.
3) Credit card accounts opened or account addressed changed.
4) Establishment of a line of credit at a store or obtaining a loan at a financial institution.
5) Goods or services purchased in their name.
6) Gaining access to secure areas.
7) Used as computer fraud.

c. Obtain or verify as appropriate identifying information of the victim to include date of birth, social security number, driver’s license number, other photo identification, current and most recent prior address, and telephone numbers.

d. Document the nature of the fraud or other crime committed in the victim’s name.

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

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

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

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

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

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

k. If not otherwise provided, document / describe the crime, the documents or information used, and the manner in which the victim’s identifying information was obtained.

l. Forward the report through the chain of command to appropriate investigative officers and immediately to intelligence agencies and federal agencies, if it appears to have national security implications.

3. Assisting Victims (CALEA 42.2.8.e)

Officers taking reports of identity theft should take those steps reasonable possible to help victims resolve their problem. This includes providing victims with the following suggestions where appropriate.

a. Contact the Federal Trade Commission (FTC) (1-800-877-IDTHEFT)-Which acts as the nation’s clearinghouse for information related to identity theft crimes – for assistance from trained counselors in resolving credit related problems.

b. Cancel each credit and charge card and request new cards with new account numbers.

c. Contact the fraud departments of the three major credit reporting agencies [Equifax (1-800-525-6285), Experian (1-888-397-3742),

POLICY AND PROCEDURE # 105 Identity Theft

4
TransUnion (1-800-680-7289)], and ask them to put a fraud alert on the account and add a victims’ statement requesting creditors to contact the victim before opening new accounts in his or her name. Also request copies of your credit report.

d. If bank accounts are involved, report the loss to each financial institution, cancel existing accounts and open new ones with new account numbers. If deemed necessary, place stop payments on outstanding checks and contact creditors to explain.

e. If a driver’s license is involved, contact the state motor vehicle department. If the driver’s license uses the social security number, request a new driver’s license number. In such cases, also check with the Social Security Administration to determine the accuracy and integrity of your account.

f. Change the locks on your house and cars if there is any indication that these have been copied or otherwise compromised.

4. Identity Theft File

The Identity Theft File will serve as a means for law enforcement to "flag" stolen identities and identify the imposter when encountered by law enforcement. When an identity theft victim becomes aware that his/her identity has been stolen and reports the incident to law enforcement, the agency's handling of the identity theft case should parallel the criteria as outlined in NCIC Operating Manual.

The Public Safety Officer should complete an incident report and collect pertinent information from the victim to create a victim profile that is entered into the Identity Theft File of NCIC. The agency enters the information only after the victim signs a consent waiver (PSD-202) (CALEA 42.2.8.b). The waiver states that the victim provides permission for the information to be entered in the Identity Theft File. It also acknowledges that the victim may withdraw the consent by providing a written request to the entering agency. At that time, the record will be canceled from the Identity Theft File.

The profile should include information such as the victim's name, date of birth, Social Security number, and the type of identity theft. In addition, a password is established either by the victim or the police officer and entered into the Identity Theft File. The password will identify the person as the victim and should be provided to the victim when the police report is filed. (The victim should retain the password to use during any potential future police encounters.) Agencies may also enter a mug shot of the victim into NCIC. The mug shot may be used as an additional form of identification for the victim. When the mug shot is retrieved, it
must clearly specify that the mug shot is that of the victim and not that of the offender.

During a subsequent encounter by law enforcement, including routine traffic stops, a person’s query into NCIC will automatically search the Identity Theft File and, if positive, generate a response to the inquiring agency. The officer will receive a response listing the victim profile, including the password, thereby providing the officer with the information necessary to verify that the person encountered is the victim or that the person may be using a false identity. The officer should be cognizant that the individual should not be arrested or detained based solely upon the information provided in the positive response from the Identity Theft File.

The response should be considered along with additional information or circumstances surrounding the encounter before the officer take action. Information on deceased persons may also be entered into the Identity Theft File. If a police officer becomes aware of a deceased person’s identity being stolen, that information can be entered into the file noting that the person is deceased.

Criteria for Entry:

An entry in the Identity Theft File must be supported by an official complaint (electronic or hard copy) recorded by and on file at a law enforcement agency. Documentation for the identity theft complaint must meet the following criteria before an entry can be made into the Identity Theft File:

a. Someone is using a means of identification of the victim (denoted in the Identity Theft and Assumption Deterrence Act of 1998 as any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual).

b. The identity of the victim is being used without the victim's permission.

c. The victim's identity is being used or intended to be used to commit an unlawful activity.

d. The victim must sign a consent waiver prior to the information being entered into the Identity Theft File. The following waiver may be used independently or incorporated into a state form.

e. Information on deceased persons may be entered into the file if it is deemed by the police officer that the victim’s information has been stolen. No consent form is required with the entry of deceased person information.
If the identity of the thief is known and an arrest warrant has been issued, the agency should enter the victim information in the S/F Fields in the Wanted Person File. Only the agency that takes the identity theft complaint may make an NCIC identity theft entry. The only exception is that any criminal justice agency or regional dispatch center may act as a holder of the record for another agency that has no telecommunications equipment. When such an entry is made, the agency holding the record may place its own Originating Agency Identifier (ORI) in the ORI Field only when there is a written agreement between the two agencies that delineates the legal responsibility of each for the record. Additional information concerning these responsibilities can be found in the ORI File Chapter of NCIC.

Procedure for MUSC Communication Center will be as follow:

Entry will only be made after the incident report, consent form and all NCIC requirements for entry are made.

MUSC Safety Identity Theft Form will be completed by the officer (PSD-203).

The entry will be logged in the Hot File (Red Binder) and paperwork will be returned to the Record’s Section to be placed into the case file.

5. Investigations (CALEA 42.2.8.d)

Investigation of identity theft shall include but not be limited to the following actions where appropriate.

a. Review the crime report and conduct any follow-up inquiries of victims or others as appropriate for clarification / expansion of information.

b. Contact the FTC Consumer Sentinel law enforcement network and search the database for investigative leads.

c. Contact other involved or potentially involved law enforcement agencies for collaboration and avoidance of duplication. These agencies include but are not limited to

d. Federal law enforcement agencies such as the U.S. Secret Service, the Federal Bureau of Investigation, and the U.S. Postal Inspection Service as appropriate whether or not the victim has filed a crime report with them.

e. Any state and / or local enforcement agency with which the victim has fled a crime report or where there is an indication that the identity theft took place.
6. Community Awareness and Prevention (CALEA 42.2.8.e)

Where reasonable and appropriate, officers engaged in public education / information forums, community crime prevention and awareness presentations or similar speaking or information dissemination efforts shall provide the public with information on the nature and prevention of identity theft.