# COVINGTON POLICE DEPARTMENT
## STANDARD OPERATING PROCEDURE

| | |
|---|---|
| **Subject: IDENTITY THEFT** | |
| **Date of Issue: 07-01-2007** | **Number of Pages: 4** |
| **Policy No. I115** | **Review Date:** |
| **Distribution: ALL** | **Revision Date:** |

**I. Purpose**

To provide guidelines to ensure that victims of identity crimes have a method to report identity crimes; to provide information and assistance to identity crimes victims that will lessen the impact of the crime; and to provide public information on the prevention of identity crimes,

**II. Statement of Policy**

It shall be the policy of the Covington Police Department to 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.

**III. Definition**

Identity Theft – The wrongful use of another person's identifying information, such as credit card, social security number, or driver's license number to commit financial or other crimes.

**IV. Georgia and Federal Law**

A. Georgia Law

The Personal Financial Security Act was codified in 1998 under Georgia Code sections 16-9-120 through 16-9-132. This code section set forth that the Governor's Office of Consumer Affairs shall maintain a repository for all complaints in the State of Georgia regarding identity fraud.

B. Federal Law

The federal Identity Theft and Assumption Deterrence Act of 1998 is codified in U.S. Code section 18 USC 1028. This law also created the Identity Theft Hotline and the Identity Theft Data Clearinghouse within the offices of the Federal Trade Commission. When consumers contact the FTC they will also be notified of their rights under the Fair Credit reporting Act, the Fair Credit Billing Act, the Truth in Lending Act, and the Fair Debt Collection Practices Act.

## V. Procedures

A. Identity theft is generally a means for committing the following types of unauthorized activities in the victim's name:

1. Credit card charges, debit card usages, ATM card withdrawals;

2. Credit card checks written against their account; credit card accounts opened or account addresses changed;

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

4. Goods or services purchased in their name;

5. Gaining access to secure areas;

6. Used as computer fraud;

7. Used to obtain employment.

B. Identity crimes often involve incidents that take place in two or more jurisdictions. Officers shall, upon request, complete an offense report when:

1. The victim of the crime is a local resident and the transaction or use of the compromised information took place in Covington; or

2. The victim of the crime is a local resident and the transaction or use of the compromised information took place in another jurisdiction; or

3. The transaction or use of the compromised information involved in the identity theft took place in Covington, regardless of the location of the victim.

C. 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. The report should include all available information, to include:

1. The specific personal information that was compromised. Examples may include: credit card accounts, banking information, and social security numbers;

2. How the victim was notified or became aware of the theft;

3. What specific activity took place as a result of the theft;

4. When and where the activity took place; and

5. Potential suspects or information concerning how the information may have been compromised.

D. A copy of all documents supporting the theft shall be marked with the case number and forwarded to CID. These documents may include: credit card statements, bank statements, credit reports, and other account statements or correspondence.

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

1. Contact the Federal Trade Commission (FTC) (1-877-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.

2. Contact the fraud departments for the three major credit reporting agencies {Equifax (1-800-525-6285), Experian (1-888-397-3742). TransUnion (1-800-680-7289)], and ask them to put a fraud alert on the account and add a victim's statement requesting creditors to contact the victim before opening new accounts in his or her name. Also, request copies of your credit report.

3. If credit cards are involved, cancel each credit card and request new cards with new account numbers.

4. If bank account information is 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.

5. If a driver's license is involved, contact the Department of Driver Services. 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.

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

7. As a part of taking the report, the officers will ask the victim if they would like to be entered in the GCIC/NCIC Identity Theft database, if so then the victim will complete the Consent Waiver (worksheet) as supplied by the reporting officer. This form, collecting relevant identifying information on the victim by which to create a profile, will be delivered to the Customer Service Representative for entry into GCIC/NCIC. A photograph of the victim should be taken and attached to the report case number for later identification confirmation. The victim will also provide a unique password, and document it on the Consent Waiver.

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

1. Review the incident report and conduct any follow-up inquiries of victims or others as appropriate for clarification/expansion of information.
2. Contact other involved or potentially involved law enforcement agencies for collaboration and avoidance of duplication. These agencies include, but not limited to:

   a. 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.

b. 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 theft took place in that respective jurisdiction.

3. Completing an investigative supplemental documenting the review and follow-up work completed on this case.

G. The department's Support Services/Community Outreach Division along with detectives from CID will provide the public with awareness programs on an as needed basis. These community crime prevention and awareness presentations are intended to provide the public with information on the nature and prevention of identity theft.

***This SOP supersedes any SOP previously issued.***

BY ORDER OF THE CHIEF OF POLICE:

Stacey L. Cotton

Stacey L. Cotton
Chief of Police