	Garner Police Department **Written Directive**
	Chapter: 800 – Operations
	Directive: 820.08 – Identity Fraud
Authorized by: Chief Brandon Zuidema	**Effective Date:** April 1, 2016
CALEA Standards: 42.2.8	**Last Revision:** July 1, 2014

820.8.1 Purpose

The purpose of this directive is to establish procedures for reporting and investigating the crimes of identity fraud and identity theft.

820.8.2 Policy

It is the policy of the Garner Police Department to;

- Take all measures necessary to record criminal complaints of identity theft,
- Assist victims in contacting relevant investigative and consumer protection agencies,
- Work with other federal, state, and local law enforcement agencies along with any other reporting agencies to identify perpetrators of identity theft, and
- Provide information and advice on rectifying problems caused by identity theft.

820.8.3 Definitions

A. Personal Identifying Information: Name, date of birth, social security or employer taxpayer identification number, address, phone number, driver's license number, identification card number, passport number, checking account number, saving account number, credit card number, debit card number, personal identification (PIN) code, electronic or Internet identification name or number, digital signature, biometric data, fingerprints, passwords, etc.

B. Types of Identity Crime include:

1. Bank Fraud: Fraudulent activity involving financial institutions such as, banks, credit unions, savings & loan institutions, and mortgage/lending companies.
2. Check Fraud: The writing of checks on closed accounts or stolen checks. Different forms of check fraud may include:
    a. Accounts with Insufficient Funds,
    b. Counterfeit Checks,
    c. Money Orders, and
    d. Travelers Checks.

3. Credit Card/Access Device Fraud (Skimming): Retrieving information encoded on the magnetic strip of a genuine credit card and encoding that information onto the magnetic strip of another credit card.

4. False Identification Fraud: The theft or misuse of personal identifiers in order to obtain identification (i.e. driver's license, state issued ID card, etc.), or to misrepresent the person's true identity.

5. Identity Theft: When a person knowingly obtains, possesses, or uses identifying information of another person, living or dead, with the intent to fraudulently represent that the person is the other person for the purposes of making financial or credit transactions in the other person's name, to obtain anything of value, benefit, or advantage, or for the purpose of avoiding legal consequences.

6. Passport/Visa Fraud: The theft or misuse of a Passport or a Visa in order to gain something of value and/or facilitate other criminal activity.

820.8.4 Officer Responsibilities (42.2.8)

A. Police personnel shall complete an incident report on all reported incidents of identity theft.

B. The following guidelines will be adhered to when documenting incidents of identity theft:

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

2. Reports should be classified as identity theft if they involve any of the following circumstances and there is an identifiable victim (or if the victim is deceased a family member) who can testify that they did not give the suspect(s) permission to use their identifying information:

   a. Credit cards, debit cards, and/or ATM cards;

   b. Credit card checks written against their 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 their name; or

   f. Computer/Internet related frauds.

3. Obtain and verify as appropriate, the identifying information of the victim to include:

   a. Date of birth,

   b. Social security number,

   c. Driver's license state and number,

   d. Current and most recent prior addresses,

   e. Telephone numbers, and

f. E-mail addresses.

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

5. 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.

6. 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.

   a. If the crime took place in another jurisdiction, assist the victim in contacting the appropriate law enforcement agency by providing the agency contact information. Do not simply refer the complainant to another agency.

   b. The assigned officer will document this type of incident in the RMS system in a "call for service" report and code it "I – Referred to other agency." The officer will document the actions he/she took in the narrative portion of the report.

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

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 the complainant with a report number.

11. Describe the crime, the documents or information used, and the manner in which the victim's identifying information was obtained.

C. Officers should consult with the District Attorney's Office prior to placing criminal charges related to Identity Fraud other than those cases where a suspect assumes the identify of another to avoid prosecution.

820.8.5 Follow-up Procedures (42.2.8)

A. 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); the FTC acts as the nation's clearinghouse for information related to identity theft crimes and provides trained counselors for resolving credit related problems.

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

3. Contact the fraud departments of the three major credit reporting agencies 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. They should also request copies of their credit report:

    a. Equifax (1-800-525-6283),

    b. Experian (1-888-397-3742), and

    c. Trans Union (1-800-680-7289).

4. 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.

5. If a driver's license is involved, contact the state motor vehicle department where the license is issued and request a new driver's license number.

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

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

1. Review the crime 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 or duplication. These agencies include but are not limited to Federal law enforcement agencies such as;

    a. U.S. Secret Service,

    b. Federal Bureau of Investigation, and

    c. U.S. Postal Inspection Service as appropriate whether or not the victim has filed a crime report with them.

3. Contact 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.

820.8.6 Laws and Resources

A. North Carolina laws related to identity theft are located in Chapter 14, section 113 of the North Carolina General Statutes, *Identity Fraud*.

B. Federal laws related to identity theft are located in USC section 1028, *Fraud and related activity in connection with identification documents, authentication features, and information*.

C. The International Association of Chiefs of Police provides additional resources to assist law enforcement agencies in the investigation of Identity Fraud. These resources can be found at http://www.theiacp.org/Identity-Crime.

820.8.7 Public Education and Awareness (42.2.8)

A. 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.

B. The Garner Police Department will periodically make its citizens aware of schemes and practices commonly used by perpetrators of identity theft. This may be accomplished through any of the following means:

1. Newspaper articles,

2. Presentations at community groups,

3. Social media, including the Department and Town social media outlets, and/or

4. Television and radio broadcasts.