Office of Legislative Research

Research Report

December 22, 2016

2016-R-0316

IDENTITY THEFT

By: Katherine Dwyer, Associate Legislative Attorney

PERSONAL IDENTIFYING INFORMATION

"Personal identifying information" is any name, number, or other information that may be used alone or with other information to identify a specific individual, including his or her:

- name;
- birth date;
- mother's maiden name;
- driver's license number;
- social security number;
- employee, employer, or taxpayer identification number;
- health insurance identification number;
- demand deposit or savings account number;
- credit or debit card number;
- alien registration or government passport number; or
- unique biometric data (e.g., fingerprints) (CGS § 53a-129a).

ISSUE

What are the processes for investigating identity theft and the associated penalties? What steps can an individual take to determine if his or her identity was stolen?

SUMMARY

Under state law, a person commits identity theft when he or she knowingly uses another person's personal identifying information (see sidebar) to obtain or attempt to obtain money, credit, goods, services, property, or medical information without the other person's consent. Both state and federal laws impose various penalties on individuals who commit identity theft.

In addition to local and state law enforcement, the federal entities that may participate in an identity theft investigation include the FBI, the IRS, and the Federal Trade Commission (FTC).

As discussed below, the Departments of Justice (DOJ) and Consumer Protection (DCP) recommend steps a person may take to determine if his or her identity was stolen, as well as measures he or she should take after making such a determination.

INVESTIGATING IDENTITY THEFT

By law, a person who believes he or she is the victim of identity theft may file a complaint reporting the

alleged violation with the law enforcement agency in his or her town. Law enforcement must accept the complaint, prepare a police report and provide the complainant with a copy, and investigate the alleged violation and coordinate the investigation with other law enforcement agencies if necessary (CGS § 54-1n). According to the Department of Emergency Services and Public Protection, another law enforcement agency could get involved under certain circumstances, including if the crime took place in more than one jurisdiction (e.g., when a credit card is used in multiple locations), or if the agency receives a request for assistance. The process for conducting investigations varies depending on the specific facts and circumstances of the case.

STATE LAW

Offenses and Penalties

State law prohibits stealing another person's identity and imposes various penalties, depending on the age of the victim and the amount of money or services obtained. Table 1 summarizes the identity theft laws and the associated penalties.

Table 1: State Laws Against Identity Theft

Statute (CGS §)	Crime	Description	Penalty
53a-129d	3rd degree identity theft	Knowingly using another person's identifying information to obtain or attempt to obtain money, credit, goods, services, property or medical information without the person's consent	Class D felony (punishable by up to five years in prison, up to a $5,000 fine, or both)
53a-129c	2nd degree identity theft	Identity theft in which the victim is (1) under age 60 and the value of the money, credit, goods, services, or property obtained is over $5,000 or (2) age 60 or older	Class C felony (punishable by up to 10 years in prison, up to a $10,000 fine, or both)
53a-129b	1st degree identity theft	Identity theft in which the victim is (1) under age 60 and the value of the money, credit, goods, services, or property obtained is over $10,000 or (2) age 60 or older and the value of the money, credit, goods, services, or property obtained is over $5,000	Class B felony (punishable by up to 20 years in prison, up to a $15,000 fine, or both)
53a-129e	Trafficking in personal identifying information	Selling, giving, or otherwise transferring an individual's personal identifying information to a third party knowing that the information has been obtained without the individual's authorization and the third party intends to use it for an unlawful purpose	Class D felony

Forfeiture

Under state law, all property and proceeds obtained through identity theft are subject to state forfeiture (CGS § 54-36o). Within 90 days of law enforcement seizing the property or proceeds, the chief state's attorney's office may petition the court to order forfeiture of the money or property. The court must identify the property owner and anyone who has interest in it and order the state to notify them by certified or registered mail.

Within two weeks after the notice, the court must hold a hearing on the petition. After the hearing, the court must issue an order, which the affected parties may appeal. Property the court orders forfeited must be sold at a public auction conducted by the Commissioner of Administrative Services. The proceeds must be used to pay:

1. the balance due on any lien the court preserved during the forfeiture proceedings;
2. any costs incurred for storing, maintaining, securing, and forfeiting the property; and
3. court costs.

Any balance must be deposited in the privacy protection guaranty and enforcement account, which was established by law for DCP to provide reimbursement to certain identity theft victims.

Under the law, no property may be forfeited to the state if the owner or lienholder did not know or could not have reasonably known that it was being used or was intended to be used in, or derived from, criminal activity (CGS § 54-36o).

FEDERAL LAW

Federal law prohibits knowingly transferring or using, without lawful authority, another person's identification with the intent to commit, aid, or abet any unlawful activity that violates federal law or is a felony under state law (18 U.S.C. § 1028(a)(7)). Generally, the penalty for this offense is up to a 15 year prison sentence, a fine, or both.

According to the DOJ, individuals who commit identity theft may be subject to other federal felony charges, including credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire

fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344). Penalties for these offenses include fines, criminal forfeiture, and, under some circumstances, up to 30 years imprisonment.

A person may also be charged with aggravated identity theft if he or she uses a stolen identity to commit other felony crimes (e.g., stealing Social Security benefits). Depending on the circumstances, the court must add from two to five years to the underlying felony sentence if the person is also convicted of aggravated identity theft (18 U.S.C. § 1028A).

IDENTIFYING IDENTITY THEFT

The DOJ advises consumers to take the following steps avoid becoming identity theft victims and quickly identify when such theft has ocurred:

1. be "stingy" about giving out personal identifying information to others regardless of the setting, unless there is reason to trust the requesting party;

2. check financial accounts and monthly credit statements regularly for unauthorized debits or charges and immediately notify the financial institution or credit card company of any discrepancies;

3. periodically obtain a personal credit report and review it for any accounts that were used or opened without authorization; and

4. maintain careful banking and financial account records (e.g., keep monthly statements and checks for at least one year).

According to DCP, an individual's identity may have been stolen if he or she:

1. fails to receive bills or other mail, which may signal an address change by the thief;

2. receives credit cards without applying for them or is denied credit for no apparent reason; or

3. receives calls or letters from debt collectors or businesses about merchandise or services the individual did not purchase.

While any of these incidents may simply be due to error, DCP suggests contacting the business directly to get more information.

ACTION STEPS

DCP advises a person who suspects that he or she is an identity theft victim to:

1. immediately report the crime to local police and ask for a police report to share with creditors;

2. keep all documentation and log all telephones made regarding the theft;

3. ask the fraud department of one of the three major credit bureaus (Equifax, TransUnion, or Experian) to flag the file with a fraud alert and include a statement that creditors should get permission from the individual before opening any new accounts (the notified bureau will contact the other two bureaus); and

4. verify the name, address, and social security number listed on his or her credit report and check for any unfamiliar items or accounts.

Additionally, after reviewing the credit report and documenting incorrect information, the person should contact:

1. his or her creditors, bank, utilities, and services companies and inform them of the identity theft;

2. the IRS if he or she suspects the stolen information may have been used in connection with tax violations;

3. the Post Office to find out if anyone has submitted any change of address forms on his or her behalf; and

4. the FTC to report the theft. (The FTC will generate an identity theft report that can be used to permanently block fraudulent information resulting from identity theft from appearing on the individual's credit report and prevent a company from collecting on debt resulting from identity theft. This report is also needed for the individual to put an extended fraud alert on his or her credit report.)

The FTC's website (identitytheft.gov) provides additional information and steps for an individual to take if his or her identity is stolen.

KD:bs