Identity Theft Crimes

Course # 3277
Revised September 2025

Identity Theft Crimes

ABSTRACT

This guide is designed to assist the instructor in developing an appropriate lesson plan to teach the course learning objectives. The learning objectives are the minimum required content of the Identity Crimes Training. This course is a TCOLE required course #3277 and was established by the legislature mandate 78R-SB473.

Note to Trainers: It is the responsibility of the training coordinator to ensure this curriculum and its materials are kept up to date. Refer to curriculum and legal resources for changes in subject matter or laws relating to this topic as well as the Texas Commission on Law Enforcement website at www.tcole.texas.gov for edits due to course review.

Target Population: Licensed law enforcement personnel in Texas.

Student Prerequisites:

- None

Instructor Prerequisites:

- Certified TCOLE Instructor and documented knowledge/training in course subject matter OR
- Documented subject matter expert

Length of Course: 3 hours minimum

Equipment:

- None

Training Delivery Method(s):

- Online
- Instructor-led, classroom-based
- Instructor-led, virtual classroom

Method(s) of Instruction:

- Lecture
- Discussion
- Scenarios

Facility Requirements:

- Standard classroom

Assessment: Assessment is required for completion of this course to ensure the student has a thorough comprehension of all learning objectives. Training providers are responsible for assessing and documenting student mastery of all objectives in this course.

In addition, the Commission highly recommends a variety of testing/assessment opportunities throughout the course which could include: oral or written testing, interaction with instructor and students, case study and scenario, and other means of testing student's application of the skills taught as the instructor or department deems appropriate.

Unless otherwise indicated, the minimum passing score shall be 70%.

Resource Materials:

- Abbott, Greg (Texas Attorney General), "A police report is crucial in cases of identity theft" Chicago Police, "Police Officer's Handbook—Identity Theft"
- Federal Trade Commission <https://www.identitytheft.gov/>
- Federal Trade Commission, "Consumer Sentinel Network-Data Book 2019". Accessed 07/30/2020. <https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf>
- Federal Trade Commission, "How to Keep Your Personal Information Secure". Accessed 09/25/2020. < https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure>
- Federal Trade Commission, "Steps". Access 08/30/2020. <https://www.identitytheft.gov/Steps>
- Identity Theft. Accessed 08/28/2020. < https://www.usa.gov/identity-theft>
- Identity Theft and Assumption Deterrence Act of 1998. Accessed 07/28/2020. <https://www.govinfo.gov/content/pkg/PLAW-105publ318/html/PLAW-105publ318.htm>
- Identity Theft Enforcement and Restitution Act of 2008. Accessed 07/28/2020. <https://www.govinfo.gov/content/pkg/BILLS-110hr5938enr/pdf/BILLS-110hr5938enr.pdf>
- Identity Theft Penalty Enhancement Act of 2004. Accessed 07/28/2020. <https://www.congress.gov/108/plaws/publ275/PLAW-108publ275.pdf>
- Insurance Information Institute, "Facts + Statistics: Identity theft and cybercrime". Accessed 07/28/2020. <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>

- Texas Business and Commerce Code. Chapter 20. Regulation of Consumer Credit Reporting Agencies.
- Texas Business and Commerce Code. Chapter 501. Protection of Driver's License and Social Security Numbers.
- Texas Business and Commerce Code. Chapter 607. Payment Card Skimmers on Motor Fuel Dispensers.
- Texas Business and Commerce Code. Sec. 607.103. Offenses; Penalties.
- Texas Code of Criminal Procedure. Art. 13.29. Fraudulent Use or Possession of Identifying Information.
- Texas Code of Criminal Procedure. Art. 13.291. Credit Card or Debit Card Abuse.
- Texas Code of Criminal Procedure. Art. 55.02, Sec. 2a. Procedure for Expunction.
- Texas Department of Public Safety, "Forgery Affidavit Form". Accessed 08/12/2020. <https://www.dps.texas.gov/docs/forgaff.pdf>
- Texas Department of Public Safety, "What to Do If You Have Become A Victim of Identity Theft". Accessed 07/28/2020.
- Texas District & County Attorneys Association, "2019-2021 Legislative Update", p. 9.
- Texas Penal Code §31.20. Mail Theft.
- Texas Penal Code §32.315. Fraudulent Use or Possession of Credit Card or Debit Card Information.
- Texas Penal Code §32.51. Fraudulent Use or Possession of Identifying Information.
- U.S. Department of Homeland Security, U.S. Secret Service, "Identity Crimes Interactive Resource Guide."
- U.S. Department of Justice, "Identity Theft: A Quiz for Consumers". Accessed 07/27/2020. <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-quiz>

Identity Theft Crimes

Learning Objectives

UNIT 1 Defining Identity Crimes

1.1 **Learning Objective:** Define identity theft and identity crime.

1.2 **Learning Objective:** Locate current statistical data regarding identity theft crimes.

1.3 **Learning Objective:** Identify the types of crimes associated with identity crimes.

1.4 **Learning Objective:** Describe the meaning of the terms identifying information and telecommunication access device.

1.5 **Learning Objective:** Identify the current trends associated with identity crimes.

UNIT 2 How Identity Crimes Occur

2.1 **Learning Objective:** Identify how identity crime is commonly perpetrated.

2.2 **Learning Objective:** Identify techniques used to procure false identification.

UNIT 3 Laws and Statutes Governing Identity Crimes

3.1 **Learning Objective:** Identify the federal statutes dealing with identity crimes.

3.2 **Learning Objective:** Identify the state statutes dealing with identity crimes.

3.3 **Learning Objective:** Define the term "security alert" and list the process of requesting a security alert according to the Texas Business and Commerce Code.

3.4 **Learning Objective:** Define the term "security freeze" and list the process of requesting a security freeze according to the Texas Business and Commerce Code.

UNIT 4 Prosecuting Identity Crimes

4.1 **Learning Objective:** List information needed for an identity crime offense report.

4.2 **Learning Objective:** Identify the governmental and business entities that are notified in identity crimes.

UNIT 5 Identity Crimes Prevention

5.1 **Learning Objective:** Identify techniques for educating victims and the general public on identity crimes.

5.2 **Learning Objective:** List guidelines for personal information protection against identity crimes.

5.3 **Learning Objective:** List the steps to take if identity crime occurs.

Identity Theft Crimes

UNIT 1. Defining Identity Crimes

INSTRUCTOR NOTE: At the beginning of the presentation, it is recommended that the instructor administer the pre-course quiz located in Appendix A: Identity Theft: A Quiz for Consumers. The students should take a few minutes to complete the quiz. After completion, the instructor should provide a brief oral review of the test answers with the class after emphasizing the fact that more detailed information on each question will be provided during the lecture.

1.1 Define identity theft and identity crime.

Identity theft is the theft of your personal information to commit fraud. This typically includes your name and other personal information (like your Social Security number) and the individual uses it without your permission to do things like open new accounts, use your existing accounts, or obtain medical services. An identity thief might even present your name and identity to law enforcement officers when he/she is arrested. Identity theft can have serious consequences for you and your family. It can negatively affect your credit, result in you being sued for debts that are not yours, result in incorrect and potentially health-threatening information being added to your medical records, and may even get you arrested.

Identity crime is the theft or misuse of personal or financial identifiers in order to gain something of value and/or facilitate other criminal activity.

1.2 Locate current statistical data regarding identity theft crimes.

INSTRUCTOR NOTE: It is the instructor's responsibility to incorporate **current** statistics into the presentation. The following websites contain current statistical data regarding identity theft:

- Insurance Information Institute: Facts + Statistics: Identity theft and cybercrime
- Federal Trade Commission: Consumer Sentinel Network

The Federal Trade Commission (FTC) states: "Identity theft happens when someone uses your Social Security number or other personal information to open new accounts, make purchases, or get a tax refund."

Identifying information can be utilized to commit various other crimes. The top five types of identity theft, as of 2019, reported by the Insurance Information Institute are:

1. Credit card fraud—new accounts
2. Miscellaneous identity theft, which include:
    - online shopping and payment account fraud

- e-mail and social media fraud
- medical service, insurance, and securities account fraud

3. Mobile telephone—new account
4. Business and personal loans
5. Auto loan or lease

In 2019, Texas was 4th on the state rank (reports per 100K Population) with 73,553 identity theft reports according the FTC Consumer Sentinel Network Data Book.

1.3 Identify the types of crimes associated with identity crimes.

In many instances an identity crime is used as a facilitator, through financing or anonymity, to commit other criminal activities such as mail theft, mail fraud, narcotics/drugs, organized crime, financial fraud (money laundering), mortgage fraud, weapons trafficking, homicide, terrorism, wire fraud, or computer crime/internet intrusions.

Identity crimes can begin with other seemingly unrelated crimes such as robbery, theft, burglary of a motor vehicle, computer intrusion, mail theft, theft of trash ("dumpster diving"), or theft of documents or information from businesses, medical facilities, or hotels, etc.

According to the FTC, special forms of identity theft also include:

- Tax identity theft
- Child identity theft
- Medical identity theft

SCENARIO: The officer stops a vehicle for a traffic violation, and the driver will be arrested for warrants. While completing an inventory of the vehicle because it will be impounded, the officer comes across numerous Texas ID cards and social security cards not belonging to the driver.

INSTRUCTOR NOTE:

- Based on the information given, have the students articulate why it would be reasonable to believe these forms of identification may have been stolen or fraudulently produced in order to facilitate other crimes.
- If the arrestee is in possession of a couple of ID cards belonging to another person, the officer needs to verify whether they are actually stolen. If no other individuals were with the arrestee, could they belong to someone the person was with previously? Did the individual claim to be at a nightclub and claim to be holding on to their friend's driver's license? This would not be considered identity theft without further evidence.

1.4 Describe the meaning of the terms identifying information and telecommunication access device.

A. Identifying information means information that alone, or in conjunction with, other information identifies a person, including a person's:

1. name and date of birth;

2. unique biometric data, including the person's fingerprint, voice print, or retina or iris image;

3. unique electronic identification number, address, routing code, or financial institution account number;

4. telecommunication identifying information or access device; and

5. social security number or other government-issued identification number.

B. Telecommunication access device means a card, plate, code, account number, personal identification number, electronic serial number, mobile identification number, or other telecommunications service, equipment, or instrument identifier or means of account access that alone or in conjunction with another telecommunication access device may be used to:

1. obtain money, goods, services, or other thing of value; or

2. initiate a transfer of funds other than a transfer originated solely by paper instrument.

SCENARIO: The officer takes a report where the victim reports his personal identifying information was used to obtain a credit card. The victim said his name was used, but with a different date of birth and social security number.

INSTRUCTOR NOTE:

- Students should recognize that the use of only an individual's name does not necessarily constitute identity theft. Another identifier such as date of birth and social security number in conjunction with the name is necessary to be a true identity theft.
- A mistake may have been made and the account may belong to another person with the same name, but without specific identifiers, it would be impossible to know for sure.

1.5 Identify the current trends associated with identity crimes.

Some of the current trends associated with identity theft involve the use of current technologies. This provides a unique challenge for consumers and law enforcement by testing their ability to keep up with technological advances and changes.

Some of the more recent scams involve stealing information by listening in on conversations made on cellular phones, surreptitiously reading other people's emails, hacking into computers, conducting telephone and email scams, and taking advantage of careless consumers' online shopping and banking.

INSTRUCTOR NOTE: Play two scam phone calls as examples as applicable. You can access and download examples from the FTC website:

- Social Security scam call man voice
- Social Security scam call women voice

Currently, the Identity Theft Resource Center, www.idtheftcenter.org, is an excellent website for obtaining information on new trends, scams, and consumer alerts on identity crimes.

UNIT 2. How Identity Crimes Occur

2.1 Identify how identity crime is commonly perpetrated.

- Identity crimes can occur if someone steals your wallet, purse, or briefcase, etc., containing your identification, Social Security card, credit cards, bankcards, or checkbook.
- Identity crimes can occur if someone steals your mail, especially your bank and credit card statements, pre-approved credit offers, new checks, and/or tax information.
- Identity thieves can complete a "change of address" to divert your mail to another location.
- Identity thieves may rummage through your trash or the trash of businesses to find personal data (also known as "dumpster diving").
- Identity thieves may fraudulently obtain your credit report by posing as a landlord, employer, or someone else who may have a legitimate need for (and legal right to) the information.
- Identity thieves can find personal information in your home.
- Identity thieves may obtain personal information that you share on the internet.
- Identity thieves can get information from the workplace, in a practice known as "business record theft," by stealing files out of offices where you are a customer, employee, patient, or student, by bribing an employee who has access to your files, or by "hacking" into electronic files.
- Some identity thieves also engage in "shoulder surfing": looking over your shoulder or from a nearby location as you enter your personal identification number (PIN) at an

automated teller machine (ATM). This practice has gone high-tech, with some thieves utilizing hidden "spy cameras" positioned near ATMs to observe or record people as they enter their PINs.

- Many criminals who want to obtain personal data from people online use a technique known as "spoofing": the creation of emails and websites that appear to belong to legitimate businesses such as established retail companies, financial institutions, and online auctions sites. Consumers receive emails from thieves claiming to be the legitimate businesses, and are directed/linked to websites that appear to be run by those businesses. The consumers are then directed to enter large amounts of personal data. The thieves sending the emails or running the websites actually have no connection with those businesses, and their sole purpose is to obtain the consumers' personal data so that they can engage in various fraud schemes.

SCENARIO: The officer receives a call to take a report on identity theft. The victim has never lost or misplaced her ID or social security card and is upset because she does not know how her information was compromised.

INSTRUCTOR NOTE:

- Begin with a discussion on other possible methods that an identity theft can occur.
- The student should be able to explain that most identity theft occurs because of current technology.
- Show an example from YouTube "How Do ATM Skimmers Work" (1:57) if applicable. Even with all of the anti-theft protection technology, criminals are increasingly finding ways to get around any blocks. Many times, there is no way to find out how the information was compromised.

2.2 Identify techniques used to procure false identification.

A wide variety of sources, including bookstores and internet retailers, provide publications that give criminals step-by-step instructions on techniques for producing false documents.

INSTRUCTOR NOTE: Show the students some of the resources that are available to criminals who want to create false documents. Incorporate news stories explaining how some suspects obtain or create false ID documents. For example:

- FTC Scam Alerts topic, video and media
- Phishing Scam Game:
  - Phishing Scams
  - Spam Scam Slam

- Videos:
    - Hang Up on Phone Fraud (3:08)
    - Online Shopping Tips (3:28)
    - Money Wiring Scams (1:30)

UNIT 3. Laws and Statutes Governing Identity Crimes

3.1 Identify the federal statutes dealing with identity crimes.

A. The 1998 Identity Theft and Assumption Deterrence Act.

The act amended Title 18, U.S. Code, Section 1028 made it a federal crime to "knowingly transfer or use, 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 violation of federal law, or that constitutes a felony under any applicable state or local law."

B. The 2004 Identity Theft Penalty Enhancement Act.

The act established penalties for "aggravated" identity theft, which is using the identity of another person to commit felony crimes, including immigration violations, theft of another's Social Security benefits, and acts of domestic terrorism. The act required the court to sentence two additional years for a general offense and five years for a terrorism offense.

C. The 2008 Identity Theft Enforcement and Restitution Act.

This act amended Title 18 U.S. Code, Section 3663(b) to make it clear that restitution orders for identity theft cases may include an amount equal to the value of the victim's time spent remediating the actual or intended harm of the identity theft or aggravated identity theft. The new law also allowed federal courts to prosecute when the criminal and the victim live in the same state. Under previous law, federal courts only had jurisdiction if the thief used interstate communication to access the victim's personally identifiable information.

3.2 Identify the state statutes dealing with identity crimes.

Texas Penal Code §32.51. Fraudulent Use or Possession of Identifying Information.

(b) A person commits an offense if the person, with the intent to harm or defraud another, obtains, possesses, transfers, or uses an item of:

(1) identifying information of another person without the other person's consent or effective consent;

(2) information concerning a deceased natural person, including a stillborn infant or fetus, that would be identifying information of that person were that person alive, if the item of information is obtained, possessed, transferred, or used without legal authorization; or

(3) identifying information of a child younger than 18 years of age.

(b-1) For the purposes of Subsection (b), the actor is presumed to have the intent to harm or defraud another if the actor possesses:

(1) the identifying information of three or more other persons;

(2) information described by Subsection (b)(2) concerning three or more deceased persons; or

(3) information described by Subdivision (1) or (2) concerning three or more persons or deceased persons.

(b-2) The presumption established under Subsection (b-1) does not apply to a business or other commercial entity or a government agency that is engaged in a business activity or governmental function that does not violate a penal law of this state.

(c) An offense under this section is:

(1) a state jail felony if the number of items obtained, possessed, transferred, or used is less than five;

(2) a felony of the third degree if the number of items obtained, possessed, transferred, or used is five or more but less than 10;

(3) a felony of the second degree if the number of items obtained, possessed, transferred, or used is 10 or more but less than 50; or

(4) a felony of the first degree if the number of items obtained, possessed, transferred, or used is 50 or more.

(c-1) An offense described for purposes of punishment by Subsections (c)(1)-(3) is increased to the next higher category of offense if it is shown on the trial of the offense that:

(1) the offense was committed against an elderly individual as defined by Section 22.04; or

(2) the actor fraudulently used identifying information with the intent to facilitate an offense under Article 62.102, Code of Criminal Procedure.

(d) If a court orders a defendant convicted of an offense under this section to make restitution to the victim of the offense, the court may order the defendant to

reimburse the victim for lost income or other expenses, other than attorney's fees, incurred as a result of the offense.

(e) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

Two other statutes in the Texas Penal Code that relate to identity crimes would be Mail Theft and Fraudulent Use or Possession of Credit Card or Debit Card Information. The mail theft statute provides punishment enhancements if the appropriated mail contained an item of identifying information and the actor committed the offense with the intent to facilitate an offense under Section 32.51. The Texas District & County Attorneys Association (TDCAA) states that, Fraudulent Use or Possession of Credit Card or Debit Card Information may overlap with several other existing crimes such as Credit Card or Debit Card Abuse or Fraudulent Use or Possession of Identifying Information. The purpose behind the creation of this new offense was to help authorities crack down on gas pump credit card skimmers (Edmonds, 2019, p. 9.)

Texas Penal Code §31.20. Mail Theft.

(a) In this section:

(1) "Disabled individual" and "elderly individual" have the meanings assigned by Section 22.04.

(2) "Identifying information" has the meaning assigned by Section 32.51.

(3) "Mail" means a letter, postal card, package, bag, or other sealed article that:

(A) is delivered by a common carrier or delivery service and not yet received by the addressee; or

(B) has been left to be collected for delivery by a common carrier or delivery service.

(b) A person commits an offense if the person intentionally appropriates mail from another person's mailbox or premises without the effective consent of the addressee and with the intent to deprive that addressee of the mail.

(c) Except as provided by Subsections (d) and (e), an offense under this section is:

(1) a Class A misdemeanor if the mail is appropriated from fewer than 10 addressees;

(2) a state jail felony if the mail is appropriated from at least 10 but fewer than 30 addressees; or

(3) a felony of the third degree if the mail is appropriated from 30 or more addressees.

(d) If it is shown on the trial of an offense under this section that the appropriated mail contained an item of identifying information and the actor committed the offense with the intent to facilitate an offense under Section 32.51, an offense under this section is:

(1) a state jail felony if the mail is appropriated from fewer than 10 addressees;

(2) a felony of the third degree if the mail is appropriated from at least 10 but fewer than 20 addressees;

(3) a felony of the second degree if the mail is appropriated from at least 20 but fewer than 50 addressees; or

(4) a felony of the first degree if the mail is appropriated from 50 or more addressees.

(e) An offense described for purposes of punishment by Subsection (d)(1), (2), or (3) is increased to the next higher category of offense if it is shown on the trial of the offense that at the time of the offense the actor knew or had reason to believe that an addressee from whom the actor appropriated mail was a disabled individual or an elderly individual.

(f) If conduct that constitutes an offense under this section also constitutes an offense under another law, the actor may be prosecuted under this section, the other law, or both.

Texas Penal Code §32.315. Fraudulent Use or Possession of Credit Card or Debit Card Information.

(a) In this section:

(1) "Counterfeit credit card or debit card" means a:

(A) credit card or debit card that:

(i) purports on its face to have been issued by an issuer that did not issue the card;

(ii) has been altered to contain a digital imprint other than that which was placed on the card by the issuer;

(iii) contains a digital imprint with account information or account holder information differing from that which is printed or embossed on the card; or

(iv) has been altered to change the account information or account holder information on the face of the card from that which was printed or embossed on the card by the issuer; or

(B) card, other than one issued as a credit card or debit card, that has been altered to contain the digital imprint of a credit card or debit card.

(2) "Credit card" and "debit card" have the meanings assigned by Section 32.31.

(3) "Digital imprint" means the digital data placed on a credit card or debit card or on a counterfeit credit card or debit card.

(b) A person commits an offense if the person, with the intent to harm or defraud another, obtains, possesses, transfers, or uses:

(1) a counterfeit credit card or debit card;

(2) the number and expiration date of a credit card or debit card without the consent of the account holder; or

(3) the data stored on the digital imprint of a credit card or debit card without the consent of the account holder.

(c) If an actor possessed five or more of an item described by Subsection (b)(2) or (3), a rebuttable presumption exists that the actor possessed each item without the consent of the account holder.

(d) The presumption established under Subsection (c) does not apply to a business or other commercial entity or a government agency that is engaged in a business activity or governmental function that does not violate a penal law of this state.

(e) An offense under this section is:

(1) a state jail felony if the number of items obtained, possessed, transferred, or used is less than five;

(2) a felony of the third degree if the number of items obtained, possessed, transferred, or used is five or more but less than 10;

(3) a felony of the second degree if the number of items obtained, possessed, transferred, or used is 10 or more but less than 50; or

(4) a felony of the first degree if the number of items obtained, possessed, transferred, or used is 50 or more.

(f) If a court orders a defendant convicted of an offense under this section to make restitution to a victim of the offense, the court may order the defendant to

reimburse the victim for lost income or other expenses, other than attorney's fees, incurred as a result of the offense.

(g) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

Texas Code of Criminal Procedure. Art. 13A.260 Fraudulent Use or Possession of Identifying Information.

An offense under Section 32.51, Penal Code, may be prosecuted in any county in which the offense was committed or in the county of residence for the person whose identifying information was fraudulently obtained, possessed, transferred, or used.

Texas Code of Criminal Procedure. Art. 13A.255. Credit Card or Debit Card Abuse.

An offense under Section 32.31, Penal Code, may be prosecuted in any county in which the offense was committed or in the county of residence for any person whose credit card or debit card was unlawfully possessed or used by the defendant.

Texas Code of Criminal Procedure. Art. 55A.256. Procedure for Expunction.

(a) A person who is entitled to expunction of information contained in records and files under Article 55A.006 may file an application for expunction with the attorney representing the state in the prosecution of felonies in the county in which the person resides.

(b) The application must be verified, include authenticated fingerprint records of the applicant, and include the following or an explanation for why one or more of the following is not included:

(1) the applicant's full name, sex, race, date of birth, driver's license number, Social Security number, and address at the time of the applicable arrest;

(2) the following information regarding the arrest:

(A) the date of arrest;

(B) the offense charged against the person arrested;

(C) the name of the county or municipality in which the arrest occurred; and

(D) the name of the arresting agency; and

(3) a statement, as appropriate, that the applicant:

(A) was arrested solely as a result of identifying information that was inaccurate due to a clerical error; or

(B) is not the person arrested and for whom the arrest records and files were created and did not give the arrested person consent to falsely identify himself or herself as the applicant.

Texas Business and Commerce Code. Chapter 20. Regulation of Consumer Credit Reporting Agencies.

Texas Business and Commerce Code. Chapter 501. Protection of Driver's License and Social Security Numbers.

Texas Business and Commerce Code. Chapter 607. Payment Card Skimmers on Motor Fuel Dispensers.

Sec. 607.103. Offenses; Penalties.

(b) A person commits an offense if the person negligently or recklessly disposes of a skimmer that was installed on the unattended payment terminal of a motor fuel dispenser by another person. An offense under this subsection is a Class B misdemeanor.

(c) A person commits an offense if, knowing that an investigation is ongoing or that a criminal proceeding has been commenced and is pending, the person disposes of a skimmer that was installed on the unattended payment terminal of a motor fuel dispenser by another person. An offense under this subsection is a felony of the third degree.

3.3 Define the term "security alert" and list the process of requesting a security alert according to the Texas Business and Commerce Code.

A. Security Alert Definition

Security alert means a notice is placed on a consumer file that alerts a recipient of a consumer report involving that consumer file that the consumer's identity may have been used without the consumer's consent to fraudulently obtain goods or services in the consumer's name.

B. Requesting a Security Alert

On a request in writing or by telephone and with proper identification provided by a consumer, a consumer reporting agency shall place a security alert on the consumer's consumer file not later than 24 hours after the date the agency receives the request. The security alert must remain in effect for not less than 45 days after the date the agency places the security alert on the file. There is no limit on the number of security

alerts a consumer may request. At the end of a 45-day security alert, or by request in writing or by telephone and with proper identification provided by the consumer, the agency shall provide the consumer with a copy of the consumer's file. A consumer may include with the security alert request a telephone number to be used by persons to verify the consumer's identity before entering into a transaction with the consumer.

3.4 Define the term "security freeze" and list the process of requesting a security freeze according to the Texas Business and Commerce Code.

A. Security Freeze Definition

Security freeze means a notice placed on a consumer file that prohibits a consumer reporting agency from releasing a consumer report relating to the extension of credit involving that consumer file without the express authorization of the consumer.

B. Requesting a Security Freeze

(a) On written request sent by certified mail that includes proper identification provided by a consumer, a consumer reporting agency shall place a security freeze on a consumer's consumer file not later than the fifth business day after the date the agency receives the request.

(b) On written request for a security freeze provided by a consumer under Subsection (a), a consumer reporting agency shall disclose to the consumer the process of placing, removing, and temporarily lifting a security freeze and the process for allowing access to information from the consumer's consumer file for a specific requester or period while the security freeze is in effect.

(c) A consumer reporting agency shall, not later than the 10th business day after the date the agency receives the request for a security freeze:

(1) send a written confirmation of the security freeze to the consumer; and

(2) provide the consumer with a unique personal identification number or password to be used by the consumer to authorize a removal or temporary lifting of the security freeze under Section 20.037.

(d) A consumer may request in writing a replacement personal identification number or password. The request must comply with the requirements for requesting a security freeze under Subsection (a). The consumer reporting agency shall not later than the third business day after the date the agency receives the request for a replacement personal identification number or password provide the consumer with a new unique personal identification number or password to be used by the consumer instead of the number or password that was provided under Subsection (c).

C. Active Duty Alerts

According to the FTC, an active duty alert adds an extra layer of protection to the credit records of servicemembers while they are deployed.

SCENARIO: A victim goes to the station to file a report for an identity theft incident. The individual wants to know how to stop anyone from using their information again.

INSTRUCTOR NOTE:

- Explain that there is no way to absolutely stop anyone from using another person's identity. Individuals can take steps to protect themselves by placing a Security Alert or Security Freeze with the credit agencies. This will alert the victim to fraudulent activity they may not be aware of and provide a mechanism for stopping unauthorized activity.
- Provide resource links with summary for answer:
  - Learn how to be a safe consumer, what to do when a purchase or service goes wrong, and more https://www.usa.gov/consumer
  - Provides identity theft resources to consumers and current scam trends https://consumer.ftc.gov/identity-theft-online-security
  - Strategy, Policy and Training of Identity theft and identity theft fraud https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

UNIT 4. Prosecuting Identity Crimes

4.1 List information needed for an identity crime offense report.

Taking a written report is vital to the victim(s) because credit bureaus require a police report in order to block fraudulent information and to begin repairing the victim's credit reports. In addition, many financial institutions require a police report with an affidavit of fraud.

INSTRUCTOR NOTE: Direct the students to Appendix B: Identity Crime Incident Detail Form. Although it is not necessary to discuss every item contained in the form, a brief explanation highlighting a few sections should be discussed with students.

A. Have the victim fill out an identity crime report. This document provides the officer/investigator with detailed information to:

1. understand the type of incident that occurred,
2. organize the investigative case,
3. determine where evidence might be found,

4. develop a theory of how the identity theft occurred, and

5. determine what financial institutions should be contacted in the course of the investigation.

B. Ask the victim to begin gathering documentation:

1. Bank and credit card statements, letters from creditors, and merchant account statements, etc.

2. Credit reports from the three major credit bureaus (Equifax, Experian, and Trans Union) and voluntarily give them to you. If not given voluntarily by the victim, a subpoena is needed from the courts to obtain victim credit histories.

SCENARIO: An officer responds to take a report on identity theft. What information needs to be gathered to assist with the investigation?

INSTRUCTOR NOTE: Place students in small groups to complete the following:

- The student should first confirm that the offense is an identity theft (similar to credit card or debit card abuse).
  - If a person's existing credit card or debit card is used for purchases, it is not an identity theft, but rather credit card or debit card abuse.
  - If a new account was opened using the victim's information without consent, it is identity theft.
- The student will determine jurisdiction, if possible, where the identity theft occurred. Remember, Texas Code of Criminal Procedure 13A.255 and 13A.260 indicates the offenses of 32.31 and 32.51 may be prosecuted in any county in which the offense was committed or in the county of the residence of the victim. What does this mean? Being a victim of identity theft and/or credit card or debit card abuse is frustrating. To prevent further frustration by being referred to an outside jurisdiction where the crime occurred, the offense report can be generated by the agency where the resident/victim resides. Be sure to follow Department policy regarding the taking of reports.
- The student will put as much information as possible in the report to include date of occurrence, account numbers, and exactly what personal identifying information was used.
- The student will request that the victim obtain documentation to assist with the case.

  Note: The student should know if the victim brings documentation with them, it may be scanned into the case. If they bring large amounts of documentation, ask the victim to keep it to provide to an investigator at a later date.

4.2 Identify the governmental and business entities that are notified in identity crimes.

A. Federal Bureau of Investigation (FBI). Notify if an identity crime is used to commit a bank fraud, governmental fraud or in furtherance of an investment scheme, insurance fraud, etc. involving losses over $100,000.

B. U. S. Secret Service (USSS). Notify if there is any custody arrest of individuals associated with identity crime or identity takeover. This would involve the seizure or recovery of any amount of identity crime devices/equipment/products such as skimmers (small electronic devices that can gather information, such as your name, address, credit limit, and PIN from your credit card); counterfeit identification documents; counterfeit credit cards; or lists of personal identifiers (e.g., names, Social Security numbers, dates of birth, bank account numbers, and credit card numbers).

C. U. S. Postal Service (USPS). Notify if an individual is taken into custody for committing a financial crime involving the U.S. mail. Postal inspectors will respond to violations relating to identity crime, forgery, credit cards and checks, mail theft, mail fraud, and internet fraud (when the scheme involves use of the U.S. mail).

D. Social Security Administration (SSA). Notify if the misuse of a Social Security number involved Social Security program fraud, or if there is either a significant financial loss to an individual or institution, or a significant number of counterfeit Social Security cards are seized.

E. Federal Trade Commission (FTC). Have identity crime victims file a report with the Federal Trade Commission. The FTC has overhauled the process for helping victims of identity theft. Individuals can go to https://www.identitytheft.gov/ to report identity theft and get a recovery plan. This plan includes the forms, affidavits, and letters needed to help guide individuals through the recovery process.

F. Texas Department of Public Safety (TxDPS). This agency is responsible for the issuance of State driver's licenses and identification cards. It is also responsible for the storage and expunction of criminal records. Contact the Texas Department of Public Safety at (512) 424-2000 and online at:
https://www.dps.texas.gov/section/crime-records-service/criminal-history-records

Note: Other state and local agencies may provide additional assistance with investigating identity crimes.

G. Consumer Credit Reporting Agencies. Tell victims to have a "fraud alert" placed on their credit reports. The fraud alert will show up on their credit report when companies make inquiries about their credit and may stop additional fraud.

The three major credit-reporting agencies are:

- Experian
  1-888-397-3742 www.experian.com
- Trans Union
  1-800-680-7289 www.transunion.com/get-credit-report
- Equifax
  1-800-525-6285 www.equifax.com

H. Financial Institutions (e.g., banks, credit card companies, and financial advisors). Advise victims to contact their financial institutions to report any suspicions of identity crime. The financial institution can check to see if there has been any unusual activity. Victims should establish strong passwords for their accounts.

I. Utility Companies (e.g., power, water, phone, and cable companies, etc.). Victims may want to contact their utility companies to report instances of possible identity crime. Utility companies can check for any unusual account activity.

UNIT 5. Identity Crimes Prevention

5.1 Identify techniques for educating victims and the general public on identity crimes.

Law enforcement agencies should be proactive in their approach to educating the public about identity crime. Current techniques used to educate the public about other crimes can be used to facilitate information on identity crimes. Some of these techniques may include public service announcements (PSAs) and community policing. Law enforcement agencies can make use of the vast amount of information already available on the internet to guide the public and victims of identity crimes.

INSTRUCTOR NOTE: Law enforcement can help identity theft victims by:

- Encouraging individuals to create an Identity Theft Report and get a personal recovery plan at IdentityTheft.gov
- Sharing free identity theft resources from the FTC
- Taking a police report if asked. Some businesses require a police report to remove fraudulent debts from a victims account.

An additional video resource that could be used is available from the FTC and is titled "5 Ways to Help Protect Your Identity" (1:26).

5.2 List guidelines for personal information protection against identity crimes.

INSTRUCTOR NOTE: Emphasize the fact that the more a person becomes aware about his/her personal and financial records the better prepared he/she will be if they become a victim of identity crime.

A. Keeping Your Personal Information Secure Offline

1. Do not give out personal information over the phone unless you initiated the contact or know who you're dealing with. This also includes written information at a workplace, a business, a child's school, and/or a doctor's office. Have them ask why the business or entity needs it, how they will safeguard it, and the consequences of not sharing their Social Security number, driver's license number, date of birth, place of birth, home address, mother's maiden name, or any password.

2. Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home.

3. Limit the amount of personal information on their checks. It is recommended that they do not put their driver's license, identification card, or Social Security number on their checks. Do not have new checks mailed to their home unless they have a secure mailbox with a lock.

4. Pay attention to their billing cycles. If bills or financial statements are late, contact the sender. Review their credit card and bank account statements carefully and often. Compare receipts with account statements. Watch for unauthorized transactions.

5. Read the statements from health care providers and health insurance company plan benefits. Make sure the claims listed and paid correlate with the care given.

6. Destroy the labels on prescription bottles before they are thrown out. Don't share health plan information with anyone who offers free health services or products.

7. Shred receipts, credit offers, credit applications, insurance forms, account statements, physician statements, checks, bank statements, expired charge cards, and similar documents, and expired credit cards. This can prevent "dumpster divers" from gaining access to personal information.

8. Secure their Social Security number. Don't carry a Social Security card in their wallet. Only give out the number when absolutely necessary. Store personal information in a safe place. Create a personal my Social Security account to help you keep track of your records and identify any suspicious activity.

B. Keeping Your Personal Information Secure Online

1. Create complex passwords that identity thieves cannot guess. Have them change passwords if a company that they do business with has a breach of its databases. It is a best practice to routinely change passwords and have different passwords for different databases.

2. Be alert to imposters and know who is gaining access to your personal or financial information. Do not give out personal information over the phone, through the mail, or over the internet unless you initiated the contact or know who you're dealing with.

3. Safely dispose of personal information when they dispose of computers, tablets, mobile devices, or other electronics. Make sure all information is saved or transfer to the new device and permanently deleted.

4. Encrypt data and keep browsers secure. Utilize encryption software that scrambles information when sent over the internet. Look for the "lock" icon in the status bar of internet browsers before sending personal or financial information online.

5. Don't overshare on social media; this may provide identity thieves with an opportunity to learn details about your life and use it to answer the 'challenge' questions on accounts and/or gain access to money and/or personal information.

C. Keeping Your Devices Secure

1. Use security software (anti-virus and anti-spyware) and a firewall. Set the preferences to either update automatically or to prompt you for updates.

2. Avoid phishing emails; do not open unknown files, click links, or download programs that you did not initiate or sent by unknowns/strangers. Opening a file or accessing an unknown item may expose your system to a virus or spyware that could capture your passwords or other information that you type.

3. Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

4. Do not keep financial information or automatic login features enabled on your laptop or mobile device. If your device is stolen, it will be harder for them to gain access to your personal information.

INSTRUCTOR NOTE: Some insurance companies offer optional coverage to their policyholders to assist them with certain expenses incurred if they become victims of identity crime.

5.3 List the steps to take if identity crime occurs.

Inform the public that they should:

A. Notify the Police or Sheriff's Office: If you believe that your identity has been fraudulently used by another person without your consent, contact your local Police Department or Sheriff's Office to file a criminal report. Document the name(s) and phone number(s) of every individual you speak to regarding the incident. List exactly what has happened, such as bad checks, credit card abuse or misuse of legal name, state driver license, or identification card. Follow up your phone calls with letters. Keep a copy of the criminal report.

B. Contact any Driver License Office: After you have filed a criminal report, you may contact any local driver license office for assistance in determining the best course of action for your individual situation. You will be asked to supply personal documentation for proof of your identity as well as criminal reports, copies of returned checks, or cancellation information on credit card or checks. You will also be asked to complete a Forgery Affidavit form that will need to be notarized. A copy of the form can be obtained at any local driver license office or printed via the online link.

C. Stolen Identity File: In 1999, the Texas Legislature charged Sheriff's Offices in Texas with the responsibility to establish a unique criminal file referred to as "The Stolen Identity File." Once the file has been established the Sheriff's Office will report the information to a statewide file managed by the Department of Public Safety. If you have any questions concerning this process, please contact your local Sheriff's Office or the Error Resolution Unit in the Crime Records Service within the Department of Public Safety at (512) 424-7256.

D. Notify Creditors and Merchants: If unauthorized charges appear on your legitimate credit cards, cancel those cards and request replacement cards with new account numbers. Cancel all unauthorized credit cards and close those accounts. Monitor credit card bills for new fraudulent activity and, if found, report it immediately to the credit card issuers and credit reporting agencies.

E. Notify Your Bank(s): Ask them to flag your account and contact you regarding any unusual activity. Take the following action in the event of such activity; if checks were stolen, place stop payment orders on them; if bank accounts were opened without your consent, close them.

F. Automatic Teller Machine (ATM) Cards: If your ATM card has been stolen or compromised, contact the issuing financial institution and request a new card, account number, and password. Do not use your old password, common passwords, or personal identification such as the last four digits of your Social Security number, your date of

birth, middle name, mother's maiden name, address or anything else that could be easily discovered.

G. Contact the Social Security Administration (SSA). Report the unauthorized use of your personal information.

- Call Office of Inspector General: (800) 269-0271 / TTY Communications 1-866-501-2101
- Submit a report online at oig.ssa.gov.
- Write: SSA Fraud Hotline, Office of the Inspector General, P.O. Box 17785, Baltimore, MD 21235
- Visit website: https://www.ssa.gov/fraud/
- You can also call SSA at (800) 772-1213 / TTY number at 1-800-325-0778 or go online to verify the accuracy of the earnings report on your SSN, and to request a copy of your Social Security Statement or get a replacement SSN Card if yours is lost or stolen.

H. Federal Trade Commission (FTC): The FTC is one place to report identity theft to the federal government. To file an identity theft complaint or request information:

- Call: (877) 438-4338; TTY: (866) 653-4261
- Write: Identity Theft Clearinghouse, FTC, 600 Pennsylvania Ave. NW, Washington, D.C. 20580
- Visit website: www.ftc.gov/idtheft

I. Notify the U.S. Passport Agency to be on alert for anyone applying for a new passport fraudulently in your name:

- Call: 1-877-487-2778 / TTY 1-888-874-7793
- Write: Use Form DS-64 and mail it to the address on the form
- Visit website: : www.travel.state.gov/passport
- Email: PassportVisaFraud@state.gov

APPENDIX A: IDENTITY THEFT: A QUIZ FOR CONSUMERS

1. When I keep my ATM cards and credit cards in my wallet, I never write my PIN (Personal Identification Number) on any of my cards.

   YES ( ) NO ( )

   REASON: If you lose your ATM or credit card, identity thieves or other criminals can have instant access to your bank or credit-card account.

2. When I leave the house, I take with me only the ATM and credit cards I need for personal or business purchases.

   YES ( ) NO ( )

   REASON: If your wallet or purse is lost or stolen, and you're carrying fewer cards, you'll have to make fewer calls to banks and credit-card companies to report the losses, and the odds of fraudulent charges in your name will be lower.

3. When I get my monthly credit-card bills, I always look carefully at the specific transactions charged to my account before I pay the bill.

   YES ( ) NO ( )

   REASON: Someone who gets your credit-card number and expiration date doesn't need the actual card to charge purchases to your account. If you don't look closely at your credit-card statement each month, you might not have any recourse if fraudulent transactions go through and you don't dispute them promptly with your credit-card company. As soon as you see unauthorized charges on your statement, contact the credit-card company immediately to report them.

4. When I get my monthly bank statements, credit-card bills, or other documents with personal financial information on them, I always shred them before putting them in the trash.

   YES ( ) NO ( )

   REASON: Some identity thieves aren't shy about "dumpster diving"—literally climbing into dumpsters or rooting through trash bins to look for identifying information that someone threw out. Buying and using a shredder on your home or office is an inexpensive way to frustrate dumpster divers and protect your personal data.

5. When I get mail saying I've been pre-approved for a credit card, and don't want to accept or activate that card, I always tear up or shred the pre-approval forms before putting them in the trash.

   YES ( ) NO ( )

   REASON: If you throw out the documents without tearing them up or shredding them, "dumpster divers" can send them back to the credit-card company, pretending to be you but

saying that your address has changed. If they can use the account from a new location, you may not know the account's being used in your name until you see it on a credit report (see below).

6. I request a copy of my credit report at least once a year.

   YES ( ) NO ( )

   REASON: Any consumer can request one free copy of his or her credit report per year. Reviewing your credit report can help you find out if someone has opened unauthorized financial accounts, or taken out unauthorized loans, in your name. Contact the three major credit bureaus: Equifax (1-800-685-1111), Experian (1-888-397-3742), or Trans Union (1-800-916-8800) to request a copy.

7. If the volume of mail I get at home has dropped off substantially, I always check with my local post office to see if anyone has improperly filed a change-of-address card in my name.

   YES ( ) NO ( )

   REASON: Some identity thieves may try to take over your credit-card and bank accounts, and delay your discovery of their criminal activities, by having your mail diverted to a new address where they can go through it without your knowledge. Your local post office should have on file any change-of-address cards, and can respond if you find that someone is improperly diverting your mail.

8. If I think that I may be a victim of identity theft, I immediately contact:

   The Federal Trade Commission to report the issue and get guidance on how to deal with it.

   YES ( ) NO ( )

   The three major credit bureaus to inform them of the situation.

   YES ( ) NO ( )

   My local police department to have an officer take a report.

   YES ( ) NO ( )

   Any businesses where the identity thief fraudulently conducted transactions in my name.

   YES ( ) NO ( )

   REASON: Identity theft is a crime under federal law, and under the laws of more than 44 states, that carries serious penalties including imprisonment and fines. To help law enforcement in investigating and prosecuting identity theft, the Federal Trade Commission (FTC) maintains a national database of complaints by identity theft victims. The FTC, through a toll-free hotline (1-877-ID-THEFT), can also help you decide what steps to take in trying to remedy the situation and restore your good name and credit. Credit bureaus should also be

notified so that they can flag your credit report. Local police, by taking a report and providing you with a copy, can help you show creditors that an identity thief has been conducting certain transactions in your name and without your permission.

INSTRUCTOR NOTE: Ask: How did you score on this quiz? If you checked even two or three of the "NO" boxes, it means that you need to take more of the precautions that are described in this course. Remember that identity thieves, unlike robbers or fraudsters, do not have to have any personal contact with you in order to commit their crimes. The more you do to protect your personal information, the lower the odds that you will become a victim of identity theft.
Source: This quiz was adapted from a U.S. Department of Justice publication available at the website: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-quiz

APPENDIX B: IDENTITY CRIME INCIDENT DETAIL FORM

IDENTITY CRIME INCIDENT DETAIL FORM

Please fill out this form and return it to the Police Department as soon as possible, or bring it to the meeting with the detective assigned to your case. The information you provide will be used to understand what occurred, organize the investigative case, determine where evidence might be found, develop a theory of how the identity crime occurred, and determine what financial institutions should be contacted in the course of the investigation.

Date this form was filled out: _____
First Name: _____
Middle Name: _____
Last Name: _____
Social Security Number: _____
Driver's License Number: _____
Date of Birth: _____
Home Address: _____
Home Telephone Number: _____
Cell Phone Number: _____
Pager Number: _____
E-Mail Address: _____
Employer: _____
Work Address: _____
Work Telephone Number: _____

1. What is the best time to reach you at home? _____
2. How did you become aware of the identity crime?

_____found fraudulent charges on my credit card bill
(Which one? _____)
_____found fraudulent charges on my cellular phone bill
(Which one? _____)
_____received bills for an account(s) I did not open
(Which one? _____)
_____found irregularities on my credit report
_____was contacted by a creditor demanding payment
(Which one? _____)

_____was contacted by a bank's fraud department regarding charges
(Which one? _____)
_____was denied a loan
_____was denied credit
_____was arrested, had a warrant issued, or a complaint filed in my name for a crime I did not commit (Which one? _____)
_____was sued for a debt I did not incur
(Which one? _____)
_____was not receiving bills regularly for a legitimate account
(Which one? _____)
_____was denied employment
_____had my driver's licenses suspended for actions I did not commit
_____received a legal filing I did not file, such as a bankruptcy
_____other (Please explain _____
_____)

3. What date did you first become aware of the identity crime? _____
4. When did the fraudulent activity begin? _____
5. What is the full name, address, birth date, and other identifying information that the fraudulent activity was made under? _____

_____

_____

6. Please list all fraudulent activity that you are aware of to date, with the locations and addresses of where fraudulent applications or purchases were made (retailers, banks, etc.). List in chronological order, if possible. For example, "On 9/18/02, I received a letter from MM Collections, stating that I had accumulated $5,000 worth of charges on American Express Account 123456789. On 9/18/02, I called American Express and spoke with Jennifer Martin. She informed me that the account was opened on 5/12/02 by telephone. I did not open this account, even though it was in my name. The account address was 123 Main St. Anytown, NE. Ms. Martin said she would send me an Affidavit of Forgery to complete and return to her." You may attach a separate piece of paper if you need the space. Please be concise and state the facts.

_____

_____

_____

_____

_____

_____

_____

_____

_____

7. What documents and identifying information were stolen and/or compromised?

_____credit card(s) (List bank(s) issuing credit cards: _____
_____)

_____ATM card (List bank issuing ATM card: _____
_____)

_____checks and/or checking account number (List bank issuing checks: _____
_____)

_____savings account passbook or number (List bank holding savings account: _____
_____)

_____brokerage or stock accounts (List banks and/or brokers: _____
_____)

_____passport (List country issuing passport: _____)

_____driver's license or license number (List state issuing license: _____)

_____state identity card or identity number (List state issuing card: _____)

_____social security card or number

_____birth certificate (List state and municipality issuing birth certificate: _____
_____)

_____resident alien card, green card, or other immigration documents

_____bank account passwords or "secret words", such as mother's maiden name

_____Other (Describe: _____
_____
_____)

_____Unknown

8. To the best of your knowledge at this point, what identity crimes have been committed?

_____making purchase(s) using my credit cards or credit card numbers without authorization

_____opening new credit card accounts in my name

_____opening utility and/or telephone accounts in my name

_____unauthorized withdrawals from my bank accounts

_____opening new bank accounts in my name

_____taking out unauthorized loans in my name

_____unauthorized access to my securities or investment accounts

_____obtaining government benefits in my name

_____obtaining employment in my name

_____obtaining medical services or insurance in my name

_____evading prosecution for crimes committed by using my name or committing new crimes under my name

_____check fraud

_____passport/visa fraud

_____other _____

9. To assist law enforcement in pinpointing when and by whom your information was compromised, it is of value to retrace your actions in recent months with regard to your personal information. This information is not solicited to "blame the victim" for the crime, but to further the investigation toward who might have stolen your personal or financial identifiers. What circumstances and activities have occurred in the last six months (include activities done by you and on your behalf by a member of your family or a friend)?

_____carried Social Security Card in my wallet

_____carried my bank account passwords, PINs, or codes in my wallet

_____gave out my Social Security Number (To whom? _____

_____)

_____my mail was stolen (When? (appx) _____)

_____I went away and my mail held at the post office or collected by someone else

_____I traveled to another location outside my home area (business or pleasure)

(Where did you go and when? _____

_____)

_____mail was diverted from my home (either by forwarding order or in a way unknown to you)

_____I did not receive a bill as usual (i.e., a credit card bill failed to come in the mail) (Which one? _____)

_____a new credit card I was supposed to receive did not arrive in the mail as expected (Which one? _____)

_____bills I was paying were left in an unlocked mailbox for pickup by the postal service

_____service people were in my home (From what company? When? _____ _____ _____)

_____documentation with my personal information was thrown in the trash without being shredded

_____credit card bills, pre-approved credit card offers, or credit card "convenience" checks in my name were thrown out without being shredded

_____my garbage was stolen or gone through

_____my ATM receipts and/or credit card receipts were thrown away without being shredded

_____my password or PIN was given to someone else

_____my home was burglarized

_____my car was stolen or burglarized

_____my purse or wallet was stolen

_____my checkbook was stolen

_____my personal information was provided to a service business or non-profit (i.e., I gave blood, donated money, took out insurance, or saw a financial planner) Please list: _____ _____

_____my credit report was queried by someone claiming to be a legitimate business interest (Who? _____)

_____I applied for credit and/or authorized a business to obtain my credit report (i.e., shopped for a new car, applied for a credit card, or refinanced a home) Please list: _____ _____

_____my personal information is available on the Internet, such as in an "open directory," "white pages," genealogy web site, or college reunion web site

_____a legitimate purchase was made where my credit card was out of my sight

_____my personal information was given to a telemarketer or a telephone solicitor

Please list: _____

_____my personal information was given to a door-to-door salesperson or charity fundraiser

Please list: _____

_____a charitable donation was made using my personal information

Please list: _____

_____my personal information was given to enter a contest or claim a prize I had won

Please list: _____

_____a new bank account or new credit card account was legitimately opened in my name

_____I re-financed my house or property (Please List _____

_____)

_____a legitimate loan was applied for or closed in my name

_____a legitimate lease was applied for or signed in my name

_____legitimate utility accounts were applied for or opened in my name

_____a license or permit was applied for legitimately in my name

_____government benefits were applied for legitimately in my name

_____my name and personal information were mentioned in the press, such as in a newspaper, magazine, or on a web site

_____online purchases were made using my credit card (Through what company? _____

_____)

_____personal information was included in an e-mail

_____I released personal information to a friend or family member

For any items checked above, please, in as much detail as possible, explain the circumstances of the situation:

_____

_____

_____

_____

_____

_____

10. How many purchases over the Internet (retailer or auction sites) have you made in the last six months? _____

11. What Internet sites have you bought from? (List all) _____

_____

_____

12. In the last six months, whom has your Social Security Number been given to? (List all)

_____

_____

_____

13. Do your checks have your Social Security Number or Driver's License Number imprinted on them?

_____Yes. (Please list retailer names where checks have been tendered)

_____

_____)

_____No.

14. Have you written your Social Security Number or Driver's License Number on any checks in the last six months, or has a retailer written those numbers on a check?

_____Yes. (Please list instances and retailer names: _____)

_____No.

15. Do you own a business(es) that may be affected by the identity crime?

_____Yes. (Please list names of businesses: _____)

_____No.

16. Do you have any information on a suspect in this identity crime case? How do you believe the theft occurred? _____

_____

17. Please list all the banks that you have accounts with. Place an (*) by accounts that have fraudulent charges on them.

Bank	*Type of account and account number (checking, savings, brokerage, pension, etc.)*	*Fraudulent charges?*

18. Please list all the credit card companies and banks that you have credit cards with. Place a (*) next to accounts that have fraudulent charges on them.

19. Please list all the utility companies you have accounts with. Place a (*) next to accounts that have fraudulent charges on them.

20. Please list all the financial institutions you have loans, leases, and mortgages from. Place a (*) next to accounts that have fraudulent charges on them.

Financial Institution	*Type of account and Account # (loan, lease, mortgage, etc.)*	*Fraudulent charges?*

21. Please list any merchants who you have credit accounts with such as department stores, or retailers? Place a (*) next to accounts that have fraudulent charges on them.

22. Please list any other financial institutions where <u>fraudulent</u> accounts were opened in your name or using your personal identifiers.

23. Please list any documents fraudulently obtained in your name (driver's licenses, social security cards, etc.)

_____

_____

_____

_____

_____

_____

_____

_____

_____

24. Have you contacted the following organizations and requested a Fraud Alert be put on your account? (Check all that you have contacted about a Fraud Alert)

_____Equifax On what date? _____

_____TransUnion On what date? _____

_____Experian On what date? _____

_____Your Bank(s) Name of Bank(s): _____

_____

_____

_____Department of Motor Vehicles

_____Social Security Administration

_____Other (Please list: _____)

25. Have you requested a credit report from each of the three credit bureaus? (Check all that you have requested a credit report from)

_____Equifax (If you have in your possession, please attach to this form)

_____TransUnion (If you have in your possession, please attach to this form)

_____Experian (If you have in your possession, please attach to this form)

26. Have you contacted any financial institution, concerning either legitimate or fraudulently opened accounts? If yes, please list:

Name of financial institution *Phone number* *Person you spoke with*

_____

_____

_____

_____

_____

_____

_____

_____

***Please bring with you to the meeting with the detective: all account statements, letters, correspondence, phone records, credit reports and other documents regarding this case.

Also, please make a copy of this completed form for your records.

Remember to keep a detailed log of all your correspondence and contacts since realizing you were the victim of identity crime.