MARYLAND POLICE AND CORRECTIONAL TRAINING COMMISSIONS

LESSON PLAN

COURSE TITLE: Police Entry-level Training Program

LESSON TITLE: Identity Theft/Fraud

PREPARED BY: James A. Durner **DATE:** 4-18-11

ADAPTED FROM: **REVIEWED/UPDATED:** 7 - 29 - 13

TIME FRAME	PARAMETERS
Suggested Length: **4.0 Hours (entry-level)** **2.0 Hours (in-service level)**	**Audience:** entry-level law enforcement recruits; or in-service personnel; **Number:** varies **Space:** classroom

TRAINING OBJECTIVES

TERMINAL OBJECTIVE: [01.07]

Given various criminal situations demonstrate the ability to identify elements of a given crime, utilizing the Annotated Code of Maryland and/or the Digest of Criminal Laws, that enable an officer to make a warrant-less arrest.

ENABLING OBJECTIVES:

Define the term IDENTITY THEFT.

Identify the basic elements of the crime of IDENTITY THEFT/FRAUD as contained in the Annotated Code of Maryland. [01.07.34]

TERMINAL OBJECTIVE: [04.04]

Identify the resources available to an officer while conducting a criminal investigation.

ENABLING OBJECTIVE:

Identify the resources available to the officer for crimes involving IDENTITY THEFT/FRAUD. [04.03.21]

EVALUATION TECHNIQUE

1. Test questions; and

2. Practical exercises/scenarios.

TERMINAL OBJECTIVE: **[04.05]**

Identify resources available to a crime victim.

ENABLING OBJECTIVE: [04.05.19]

Identify resources available to the victim for crimes involving IDENTITY THEFT/FRAUD.

TERMINAL OBJECTIVE: **[04.23]**

Identify the basic responsibility of the officer when Investigating the crime of identity theft.

TERMINAL OBJECTIVE: **[07.05]**

Demonstrate completion of acceptable police reports for various offenses/incidents/situations.

ENABLING OBJECTIVE:

Apply the law as contained in the Annotated Code of Maryland Criminal Law that requires a law enforcement officer to prepare and file a report from the victim of IDENTITY THEFT/FRAUD.

Given a scenario involving IDENTITY THEFT/FRAUD, compose a complete initial IDENTITY THEFT/FRAUD offense report that includes, at a minimum, the following elements:

- complete victim information at the time the identity theft/fraud occurred;
- complete description of the type of personal identifying information, item or document that was stolen/compromised;
- specific information about how the stolen/compromised identity information, item or document was discovered by the victim and how the identity information, item or document was used;
- potential suspect information;
- action the victim has taken to mitigate the identity loss/compromise; and
- a description of any recommended follow-up action suggested/relayed to the victim.

TERMINAL OBJECTIVE: **[08.01]**

Define crime prevention.

ENABLING OBJECTIVES:

Identify several types of personal identifying and/or financial information that may be stolen or compromised to include, at a minimum:

- personal identifiers such as:
  - name;
  - date of birth;
  - address;
  - mother's maiden name;
- credit/debit/checking/savings/ other existing financial accounts;
- account access codes/passwords;
- social security number;
- medical records;
- driver's license number or identification number;
- educational background/records; and
- computer passwords.

Identify several examples of the crime of IDENTITY THEFT/FRAUD to include, at a minimum, the theft/fraudulent use of:

- existing credit/debit cards/financial accounts to obtain goods or services;
- other financial records/personal financial information to obtain credit or other financial assistance;
- personal information to obtain various services such as medical treatment, government/social services, educational assistance, etc; and
- personal information to obtain government identity cards, licenses/other official documents.

Identify several different ways in which personal information including financial information may be stolen/compromised, to include at a minimum:

- the use of home computers;
- discarded/stolen mail;
- discarded personal/financial records; and
- theft/compromise during ***legitimate*** use of the information by a victim during a third party transaction.

Identify several different ways by which an individual can safeguard his/her personal identifying information.

INSTRUCTOR MATERIALS	
____ Overheads ____ Slides __x__ Power point presentation ____ Posters _____ _____	Videotapes: _____ _____ Reference Documents: _____ _____

EQUIPMENT / SUPPLIES NEEDED	
____ Easel Pad & Stands ____ Chart Markers ____ Masking Tape ____ Whiteboard ____ Overhead Projector ____ Projector Screen	____ Videotape Player ____ Video camera ____ Televisions ____ Video show __X__ Computers

STUDENT HANDOUTS	
# Needed	Title
	As determined by Instructor

METHODS/TECHNIQUES
Lecture - facilitated discussion – practical exercises/scenarios.

REFERENCES

"Identity Theft: What to Do If It Happens to You" Maryland Attorney General's Office, Consumer Protection Division; www.oag.state.md.us

Identity Theft Victim Assistance Training Manual, Edition 1.1, National Organization for Victim Assistance, 2010.

"Federal Trade Commission – 2006 Identity Theft Survey Report," November 2007.

"Identity Theft: What It's All About" Federal Trade Commission, June 2005.
"Filing a Complaint with FTC – Deter, Detect, Defend, Avoid ID Theft" www.ftc.gov/bcp/edu.
"Identity Theft Victim's Universal Complaint Form" (FTC) www.ftc.gov/idtheft
"Take Charge: Fighting Back Against Identity Theft" www.ftc.gov/idtheft

"Combating Identity Theft – A Strategic Plan" President's Identity Theft Task Force, April 2007.

Training Key: Identity Crime, Part I and Part II, International Association of Chiefs of Police, 2008.

"Identity Crime" Concepts and Issues Paper – IACP National Law Enforcement Policy Center, revised May 2008.

Maryland Criminal Law - Annotated

"Identity Theft Reported by Households, 2007" National Crime Victimization Survey, 2007, U.S. Department of Justice, Bureau of Justice Statistics www.ncjrs.gov

"Victims of Identity Theft, 2008" National Crime Victimization Survey Supplement, U.S. Department of Justice, Bureau of Justice Statistics www.ncjrs.gov

"Identity Theft" by Graeme R. Newman, U.S Department of Justice, Office of Community Oriented Policing Services, 2004; www.cops.usdoj.gov

www.ojp.usdoj.gov/programs/identitytheft

www.ftc.gov/sentinel

www.idsafety.org

www.privacyrights.org

"Javelin Study Finds Identity Fraud Reached New High in 2009 but Consumers are Fighting Back" news release, February 10, 2010 - Javelin Strategy and Research, www.javelinstrategy.com/news

Identity Theft Assistance Center (ITAC) www.identitytheftassistance.org

National Organization for Victim Assistance (NOVA) www.trynova.org

"Identity Theft in Maryland – Shifting Circumstances & Continuing Challenges" State of Maryland Department of Legislative Services – Office of Policy Analysis, 2013.

COMMENTARY

Every day, an increasing number of Americans discover that their identities have been compromised, often in ways and to an extent that they could not have imagined. Once they discover that their identity has been compromised and their good name and credit have been fraudulently used by someone else a sense of anger, frustration and hopelessness invades their psyche. They discover that their lives have been disrupted beyond their imagination.

Identity theft – the misuse of another individual's personal information to commit fraud – is widely considered as the fastest growing crime in America. Identity theft can happen in a variety of ways but the basic elements are the same. Criminals first gather personal information using a variety of methods. They then either sell the information to others who use the information to fraudulently obtain money, credit, goods, services or other items of value or the thief, him/herself, uses the compromised information to do likewise.

Data thieves open new credit accounts, access existing accounts, obtain government benefits or services or use a new identity to evade law enforcement. Individuals usually only learn that they have become victims of identity theft after being denied credit, being denied employment, when a debt collector seeks payment for a debt the victim did not incur or when, in some extreme situations, they are arrested for a crime that someone else has committed using their personal identifying information.

This lesson plan is *not* meant to be a complete primer on the investigation of identity theft/fraud crimes. It is intended to provide basic training about identity theft to those law enforcement officers who are the first to respond to a call from an individual who believes he/she is the victim of identity theft.

Because of the complexity of most crimes involving identity theft/fraud, the investigation into them usually requires specialized training. Identity theft crime investigations often require time, resources and expertise that most law enforcement officers do not have. Several federal agencies such as the United States Attorney General's Office, the Federal Bureau of Investigation, the Secret Service and the Federal Trade Commission offer specialized, in-depth training to law enforcement officers who are responsible for the investigation of identity theft crimes.

This lesson plan is primarily directed at officers who respond to the identity theft victim's initial call for service to take the initial crime report. It has a four-fold purpose:

- to provide officers with a basic understanding of the crime of identity theft/fraud including its scope and likely effect on victims;
- to present the elements of Maryland Criminal Law as it pertains to Identity Theft/Fraud;
- to identify the appropriate information that officers need to gather from victims of identity theft and include that information in their initial crime report both to assist the criminal investigators who will be responsible for following-up this crime and to provide valuable criminal intelligence to other law enforcement agencies who may be investigating similar/related crimes; and
- to provide officers with meaningful information that they can share with the victims of identity theft so that the victims can begin to take the necessary steps to deal with the after effects of this crime and to help them as they attempt to regain their identity.

LESSON PLAN: IDENTITY THEFT/FRAUD

PRESENTATION GUIDE	TRAINER NOTES
INTRODUCTORY SET (ANTICIPATORY SET): Every day, an increasing number of Americans discover that their identities have been compromised, often in ways and to an extent that they could not have imagined. Once they discover that their identity has been compromised and their good name and credit have been fraudulently used by someone else a sense of anger, frustration and hopelessness invades their psyche. They discover that their lives have been disrupted beyond their imagination. Identity theft – the misuse of another individual's personal identifying information to commit fraud – is widely considered as the fastest growing crime in America. Identity theft can happen in a variety of ways but the basic elements are the same. Criminals first gather personal information using a variety of methods. They then either sell the information to others who use the information to fraudulently obtain money, credit, goods, services or other items of value or the thief, him/herself, uses the compromised information to do likewise. Data thieves open new credit accounts, access existing accounts, obtain government benefits or services or use a new identity to evade law enforcement. Individuals usually only learn that they have become victims of identity theft after being denied credit, being denied employment, when a debt collector seeks payment for a debt the victim did not incur or when, in some extreme situations, they are arrested for a crime that someone else has committed using their personal identifying information. This lesson plan is *not* meant to be a complete primer on the investigation of identity theft/fraud crimes. It is intended to provide basic training about identity theft to those law enforcement officers who are the first to respond to a call from an individual who believes he/she is the victim of identity theft. The information contained in this lesson plan is also intended to provide information about identity theft and its prevention to law enforcement personnel so that they can incorporate prevention strategies into their personal lives to lessen the likelihood that they, or a family member, will become victims of this type of crime.	**Instructor Note:** **This lesson plan is intended to provide law enforcement officers with a basic understanding of Identity Theft/Fraud. It is geared towards law enforcement recruits but can easily be adapted for in-service training classes.** **It is not intended as training for investigators who specialize in the investigation of identity theft/fraud crimes.** **Training for those individuals should be obtained from sources that offer specialized training in the investigation of identity theft crimes such as the Federal Bureau of Investigation, the United States Secret Service or the Federal Trade Commission or other entities that focus on these types of crimes.** **In addition, this lesson plan is designed to provide law enforcement personnel with information regarding identity theft/fraud which they may find useful in their personal lives.**

Because of the complexity of most crimes involving identity theft, the investigation into them usually requires specialized training. Identity theft crime investigations often require time, resources and expertise that most law enforcement officers do not have. Several federal agencies such as the United States Attorney General's Office, the Federal Bureau of Investigation, the Secret Service and the Federal Trade Commission offer specialized, in-depth training to law enforcement officers who are responsible for the investigation of identity theft crimes.

This lesson plan is primarily directed at officers who respond to the identity theft victim's initial call for service to take the initial crime report. It has a four-fold purpose:

- to provide officers with a basic understanding of the crime of identity theft including its scope and likely effect on victims;
- to present the elements of Maryland Criminal Law as it pertains to identity theft/fraud;
- to identify the appropriate information that officers need to gather from the victims of identity theft and to include that information in their initial crime report both to assist the criminal investigators who will be responsible for following-up this crime and to provide valuable criminal intelligence to other law enforcement agencies who may be investigating similar/related crimes; and
- to provide officers with meaningful information that they can share with victims of identity theft so that the victims can begin to take the necessary steps to deal with the after effects of this crime and to help them as they attempt to regain their identity.

This lesson plan will present an overview of Identity Theft/Fraud, highlight Maryland Criminal Law as it relates to the investigation and reporting of crimes involving identity theft and provide victim assistance information.

Training Objectives:

TERMINAL OBJECTIVE: [04.07]
Given various criminal situations demonstrate the ability to identify elements of a given crime, utilizing the Annotated Code of Maryland Criminal Law and/or the Digest of Criminal Laws that enable an officer to make a warrantless arrest.

Define the term **IDENTITY THEFT.**

(PPT SLIDES # 2-5)

Instructor Note:

The TERMINAL training objectives listed in this lesson plan are from the entry-level law enforcement officer training program approved by the Maryland Police Training Commission. The ENABLING training objectives, where noted, are also from the law enforcement officer entry-level training program. ENABLING training objectives that do not have an objective number have been specifically developed for this lesson plan.

Identify the basic elements of the crime of IDENTITY THEFT or FRAUD as contained in the Annotated Code of Maryland Criminal Law. [01.07.34] **TERMINAL OBJECTIVE: [04.03]** **Identify the resources available to the officer while conducting a criminal investigation.** Identify the resources available to the officer for crimes involving IDENTITY THEFT/FRAUD. [04.03.21] **TERMINAL OBJECTIVE: [04.05]** **Identify resources available to a crime victim.** Identify resources available to the victim for crimes involving IDENTITY THEFT/FRAUD. [04.05.19] **TERMINAL OBJECTIVE: [04.23]** **Identify the basic responsibility of the officer when Investigating the crime of identity theft.** **TERMINAL OBJECTIVE: [07.05]** **Demonstrate completion of acceptable police reports for various offenses/incidents/situations.** Apply the law as contained in the Annotated Code of Maryland Criminal Law that requires a law enforcement officer to prepare and file a report from the victim of IDENTITY THEFT/FRAUD. Given a scenario involving identity theft/fraud, compose a complete initial identity theft/fraud offense report that includes, at a minimum, the following elements: ▪ complete victim information at the time the identity theft/fraud occurred; ▪ complete description of the type of information, item or identity document stolen/compromised; ▪ specific information about how the stolen/compromised information/identity item/document was discovered by the victim and how the identity item/document was used; ▪ potential suspect information; ▪ action that the victim has taken to mitigate the identity loss/compromise; and ▪ description of recommended follow-up action given to the victim.	**The sections of the lesson plan that meet these entry level training objectives are noted under *Instructor Notes*.** **Instructor Note:** **It is recommended that instructors use the uniform identity theft/fraud report contained in this lesson plan as a template for any identity theft report writing exercise unless their agency has adopted its own version of form for reporting identity theft/fraud.**

TERMINAL OBJECTIVE: **[08.01]**

Define crime prevention.

Identify several types of personal/financial information that may be stolen/compromised to include, at a minimum:

- personal identifiers:
  - name;
  - date of birth;
  - address;
  - mother's maiden name;
- credit/debit/checking/savings/other existing financial accounts;
- account access codes/passwords;
- social security number;
- medical records;
- driver's license number or identification number;
- educational background/records; and
- computer passwords.

Identify several examples of the crime of identity theft/fraud to include, at a minimum, the theft/fraudulent use of:

- existing credit/debit cards/financial accounts;
- other financial records/personal financial information to obtain credit or other financial assistance;
- personal information to obtain various services such as medical treatment, government/social services, educational assistance, etc; and
- personal information to obtain government identity cards, licenses or other official documents.

Identify several different ways in which personal information including financial information may be stolen/compromised, to include at a minimum:

- the use of home computers;
- discarded/stolen mail;
- discarded personal/financial records; and
- theft/compromise during *legitimate* use of information by victim during a third party transaction.

Identify several different ways by which an individual can safeguard his/her personal identifying information.

II. INSTRUCTIONAL INPUT (CONTENT):

(PPT SLIDES # 6-11)

IDENTITY THEFT (FRAUD)

OVERVIEW/BACKGROUND:

✓ **GENERAL DEFINITION – *IDENTITY THEFT/FRAUD*:**

→ The Federal Trade Commission has defined **IDENTITY THEFT/FRAUD** as:

► **THE ILLEGAL USE (WITHOUT CONSENT) OF ANOTHER'S PERSONAL IDENTIFYING INFORMATION SUCH AS:**

- CREDIT CARD NUMBERS;
- FINANCIAL RECORDS;
- SOCIAL SECURITY NUMBER;
- DRIVER'S LICENSE NUMBER;
- OTHER PERSONAL INFORMATION;

TO GAIN SOMETHING OF VALUE OR FACILITATE OTHER CRIMINAL ACTIVITY.

§ CR 8-301. IDENTITY FRAUD.

(a) ***Definitions.***

(1) In this section the following words have the meanings indicated.

(5) (i) **"PERSONAL IDENTIFYING INFORMATION"** includes:

- → name;
- → address;
- → telephone number;
- → driver's license number;
- → Social Security number;
- → place of employment;
- → employee identification number;
- → health insurance identification number;
- → medical identification number;
- → mother's maiden name;
- → bank/other financial institution account number;
- → date of birth;
- → personal identification number;
- → unique biometric data including fingerprint, voice print, retina or iris image or other unique physical representation;
- → digital signature;
- → credit card number; or
- → other payment device number.

(PPT SLIDE # 7)

Instructor Note:

A general definition of IDENTITY THEFT is presented at the beginning of this lesson plan for discussion purposes.

Additionally, the meaning of the term IDENTITY THEFT as presented in the Maryland Annotated Code of Criminal Law is also presented at this time.

TRAINING OBJECTIVE:

Define the term IDENTITY THEFT.

(PPT SLIDE # 9)

(b) ***PROHIBITED – OBTAINING PERSONAL IDENTIFYING INFORMATION WITHOUT CONSENT.***

A person may ***NOT*** KNOWINGLY, WILLFULLY, AND WITH FRAUDLENT INTENT:

- → POSSESS
- → OBTAIN, or
- → HELP ANOTHER PERSON TO POSSESS/OBTAIN ANY PERSONAL IDENTIFYING INFORMATION OF AN INDIVIDUAL:
- → *WITHOUT THE CONSENT OF THE INDIVIDUAL*

IN ORDER TO:

► USE ► SELL ► TRANSFER THE INFORMATION TO GET A:

- → BENEFIT;
- → CREDIT;
- → GOOD;
- → SERVICE; or
- → OTHER THING OF VALUE; or
- → ACCESS HEALTH INFORMATION OR HEALTH CARE IN THE NAME OF THE INDIVIDUAL.

(c) ***PROHIBITED – ASSUMING IDENTITY OF ANOTHER.***

A person may ***NOT*** KNOWINGLY AND WILLFULLY ASSUME THE IDENTITY OF ANOTHER, INCLUDING A FICTITIOUS PERSON:

(1) TO AVOID IDENTIFICATION, APPREHENSION, OR PROSECUTION FOR A CRIME; or

(2) WITH FRAUDULENT INTENT TO:

(i) GET A BENEFIT, CREDIT, GOOD, SERVICE, OR OTHER THING OF VALUE;

(ii) ACCESS HEALTH INFORMATION OR CARE;

(iii) AVOID THE PAYMENT OF DEBT OR OTHER LEGAL OBLIGATION.

FACTORS THAT CONTRIBUTE TO IDENTITY THEFT:

✓ identity theft is a relatively easy crime to commit and can occur in one or more of the following ways because individuals:

- → fail to adequately safeguard their own personal data;
- → carry personal information in wallets/purses which can be relatively easily stolen/lost:
  - ► driver's license;
  - ► credit cards;
  - ► medical insurance cards;
  - ► social security cards; etc.

(PPT SLIDE # 10)

(PPT SLIDE # 11)

Instructor Note:

§ 8-301 (c) was amended by the Maryland General Assembly in its 2011 session to include the words "ASSUMING A FICTITIOUS IDENTITY" to obtain goods/services, etc.

That prohibition BECAME EFFECTIVE OCTOBER 1, 2011.

(PPT SLIDES # 12-14)

Instructor Note:

Because law enforcement officers may find that they or a family member has become the victim of identity theft some general background information is provided in this lesson plan for their use.

→ have a relatively casual attitude about sharing personal Information with others:
  - ► frequently provide personal information to others without asking:
    - ✶ "why is the information needed?"
    - ✶ "how will the information be used?"
    - ✶ "how will the information be protected?"

→ maintain personal information on home or business computers that can be compromised by "internet burglars"/hackers or accessed by unauthorized persons;

→ unwittingly/unthinkingly discard trash/recyclable materials that contain personal information:
  - ► *dumpster diving;*

→ personal information is contained in readily accessible business/work files that are not properly safeguarded;

→ individuals/organizations/institutions entrusted with the personal data of others fail to safeguard that data:
  - ► medical records;
  - ► academic records;
  - ► employment records; etc.

→ personal identifying information can be stolen/compromised during legitimate transactions:
  - ► *skimming;*

→ personal information can frequently be transported by those responsible for its security on computers/data storage devices which can be stolen/compromised;

→ availability of personal information on Internet sites that are not protected or whose security has been breached or otherwise compromised;

→ availability of websites that offer guides to others on how to create alternative IDs and to access the personal identification information of others:
  - ► www.docusearch.com/overture
  - ► www.affordable.com/bestsellers

→ victims do not typically discover the crime until some time after it has occurred – months in some cases or years in other cases;

→ familiarity between victim and offender provides different opportunities for identity theft:
  - ► availability of personal information among relatives/coworkers/acquaintances;

→ personal information is sold/freely provided by businesses/organizations that have been given personal information during the course of legitimate transactions, including some governmental agencies:
  ► *data mining;*

→ the relative ease by which personal identifiers such as a mother's maiden name/home address/date of birth, etc., can be obtained:
  ► birth certificate/death certificate/other vital records:
    ✶ normally require one form of identification that can be forged/otherwise altered;

COMMON SOURCES CONTAINING PERSONAL IDENTIFYING INFORMATION: (PPT SLIDES # 15-16)

✓ some/all personal identifiers are commonly included in:

► PUBLIC/GOVERNMENT RECORDS:
- ✶ birth certificate
- ✶ marriage license
- ✶ divorce records
- ✶ driver's license
- ✶ vehicle registration
- ✶ voting records
- ✶ property records
- ✶ death certificates
- ✶ arrest records
- ✶ court records

► SCHOOL RECORDS:
- ✶ primary/secondary/trade
- ✶ college

► MILITARY SERVICE RECORDS:

► EMPLOYMENT FILES:
- ✶ employment application
- ✶ background/references
- ✶ medical/drug screening
- ✶ payroll
- ✶ emergency notification

► MEDICAL RECORDS:
- ✶ doctor's office
- ✶ hospital/emergency room
- ✶ immediate care facilities
- ✶ pharmacies/clinics
- ✶ self-diagnosis websites

► MAIL:
- ✶ bills/financial statements
- ✶ junk
- ✶ charitable solicitations
- ✶ pre-approved credit offers

► TRASH/RE-CYCLABLES:
- ✶ discarded but NOT DESTROYED financial statements/bills/other personal documents;

► PERSONAL/BUSINESS COMPUTERS/ELECTRONIC DEVICES;

WHAT IS STOLEN – TYPES OF INFORMATION:

✓ a variety of personal identifying information can be stolen or compromised including, but not limited to, the following:

- → personal identifiers such as:
  - ► name;
  - ► date of birth;
  - ► home address/telephone number;
  - ► physical description;
- → Social Security Number;
- → driver's license number;
- → credit/debit/bank cards and account numbers:
  - ► account passwords/access codes;
- → mail:
  - ► bank statements;
  - ► statements from other financial institutions:
    - ● retirement fund statements;
  - ► credit card statements;
  - ► pre-approved credit card offers;
  - ► telephone calling cards;
  - ► cell phone bills and utility statements with account numbers;
  - ► tax information:
    - ● employee 1099 forms;
    - ● refund checks;
- → discarded items/trash/recyclables;
- → personal or financial information by ***TRICKERY***:
  - ► Internet:
    - ● hacking:
      - ■ passwords;
    - ● unsolicited "e" mail/attachments;
    - ● free downloads of programs;
- → purchasing personal information from inside sources (employees) such as applications for goods/services/credit;
- → medical records:
  - ► medical insurance information;
- → academic records;
- → public records/documents;

(PPT SLIDES #17-18)

TRAINING OBJECTIVE:

Define crime prevention.

Identify several types of personal/financial information that may be stolen/compromised to include, at a minimum:

- credit, debit, checking, savings and other existing financial accounts;
- account access codes or passwords;
- social security number;
- medical records;
- driver's license number or identification number;
- educational background/records; and
- computer passwords.

EXAMPLE - MEDICAL RECORDS:

✓ considered by most people to be highly sensitive and deserving of the strongest protection under the law;

✓ medical records are created when you receive treatment from a health care professional and may include:
- → medical history about lifestyle:
  - ✶ use of tobacco;
  - ✶ alcohol use;
  - ✶ drug use;
- → family medical history;
- → laboratory test results;
- → medications prescribed;
- → results of operations/medical procedures;
- → results of genetic testing;
- → results of participation in research projects;
- → information provided on disability, life or accidental insurance applications;

✓ medical records are shared by a wide variety of people both in and out of the health care industry and access to those records is usually obtained by agreement to share information in return for a particular service:
- → insurance companies:
  - ✶ health/life insurers;
- → government agencies:
  - ✶ Worker's Compensation;
  - ✶ Medicare;
  - ✶ Social Security Disability;
- → Medical Information Bureau (MIB):
  - ✶ a consumer reporting agency subject to the Fair Credit Reporting Act (FCRA);
  - ✶ central database of medical information shared by insurance companies:
    - approximately 15 million individuals are on file;
    - about 600 insurance firms use MIB to obtain information about policy applicants:
      - information provided by applicants on policy applications or during pre-approval examinations are submitted/stored in MIB;
  - ✶ used when individuals apply for individual/private life/health insurance;
  - ✶ uses 230 codes to identify specific medical conditions/lifestyle choices such as smoking, alcohol or drug use or sports activities such as skydiving that the insurance industry believes are significant;
  - ✶ NOT SUBJECT TO HIPAA;

(PPT SLIDES # 19-30)

Instructor Note:

This section of the lesson plan is intended to present two examples of records that contain various items of personal identifying information:

- MEDICAL RECORDS
- PUBLIC RECORDS.

Both types of records can be readily accessed either legally or illegally by individuals intent on obtaining the personal identifying information of others.

Because MEDICAL RECORDS are so sensitive to most individuals both the federal and state privacy requirements regarding those records are presented for informational purposes.

Reference source:

www.privacyrights.org

→Prescription drug purchase and use databases:
- ✶ databases that report prescription drug purchase histories to insurance companies:
  - • may go back 5 years detailing drug usage/dosage/refills;
- ✶ database use only came to light by consumers in 2007;
- ✶ primarily used when individuals seeking private insurance;
- ✶ covered by Fair Credit Reporting Act (FCRA);
- ✶ if denied coverage, individual is entitled to the report furnished to the insurance company;
  - • if requested, report to be made available to individual 1x per year;

→ EMPLOYERS may obtain medical records by:
- ✶ asking applicants/employees to authorize disclosure of medical records:
  - • pre-employment physical exam;
  - • annual physical exams;
  - • promotional physical exams;
  - • random drug screening;
  - • worker's compensation exams;
  - • fitness for duty examinations:
    - ▪ physical;
    - ▪ mental health [psychological];
- ✶ Americans with Disabilities Act (ADA) may govern use and extent of type of questioning and exam allowed;

→ subpoenaed for court/administrative hearings:
- ✶ usually limited to relevant medical history:
  - • relevancy may be determined by judge:
    - ▪ may become public record unless sealed by the court;

→ law enforcement:
- ✶ for criminal investigation purposes;

→ direct marketers:
- ✶ when individuals participate in informal health screenings at health fairs, etc.:
  - • information may be included in databases available to sponsoring companies that have related products to sell;

→ Internet sites:
- ✶ self-help/self-diagnosis websites:
  - • no guarantee that any information that is disclosed will remain private;

✓ **Health Insurance Portability and Accountability Act (HIPAA) enacted in 2003 sets the national standard for privacy of health information:** → **sets the "floor" on medical record privacy rights:** ★ **states are free to set more stringent standards;** → **applies to medical records that are transmitted by electronic form and maintained by:** ★ **health care providers;** ★ **health care plans;** ★ **health clearinghouses;** → **a great deal of health-related information exists *outside* of health care facilities/files of health care plans:** ★ **life insurance companies;** ★ **workers compensation;** ★ **internet self-help sites;** ★ **entities conducting health care screenings such as pharmacies, shopping centers, health fairs, etc.;** → **health information provided in employment files and/or school records, including children's school records;** ✓ **FINANCIAL RECORDS maintained by some financial companies, such as insurance companies, may contain medical information which can be shared with other companies such as banks provided individuals are:** → **notified of information-sharing practices;** → **given the opportunity to opt out of information sharing;** ★ **not covered by HIPAA;** → **EXAMINE THE PRIVACY NOTICES OF FINANCIAL INSTITUTIONS CAREFULLY;** ✓ **EDUCATIONAL RECORDS maintained by schools may include a child's/individual's:** → **vaccination history:** → **allergies;** → **physical examinations for sports;** → **counseling for behavioral problems;** → **learning disabilities;** → **visits to the school nurse;** ★ **covered by Family Educational Rights and Privacy Act (FERPA) not HIPAA;** ✓ **ELECTRONIC HEALTH RECORDS (EHRs):** → **government-promoted system that allows health care providers to consolidate/store/retrieve/share medical information about an individual's entire medical history:** ★ **$19 billion allocated in 2009 American Recovery and Reinvestment Act (Stimulus Law);**	**(PPT SLIDE # 22)**

✓ **PERSONAL HEALTH RECORDS (PHRs):**

→ commercial systems for storing medical records:
- ✶ operated by Internet vendors:
  - • allow consumers to create their own medical history;

→ commercial "custodian" of the records **NOT** necessarily covered by HIPAA:
- ✶ records privacy ***NOT*** assured/guaranteed;

✓ **EMPLOYMENT RECORDS** may contain information related to:
- → Occupational Safety and Health Act (OSHA);
- → Family and Medical Leave Act (FMLA);
- → agency sponsored health and fitness programs:
  - ✶ Employee Health Programs (EHP):
    - • weight loss;
    - • exercise;
  - ✶ blood pressure/diabetes/cardio-vascular screenings;
- → FITNESS FOR DUTY EXAMINATIONS:
  - ✶ physical;
  - ✶ mental health [psychological];
- → counseling for personal/family problems (EAP);
  - ✶ substance abuse counseling
    - • MAY NOT BE COVERED BY HIPAA;

MARYLAND LAW REGARDING MEDICAL RECORDS:

Code of Maryland
Health – General
Title 4
Statistics and Records
Subtitle 3 – Confidentiality of Medical Records
[HG § 4-301 et al.]

✓HG § 4-301 defines among other things:
- → "health care"
- → "health care provider"
- → "medical record"
- → "mental health services"
- → "patient"
- → "person of interest"
- → "primary provider of mental health services"
- → "recipient"

(PPT SLIDES # 24-30)

Instructor Note:

An overview of Maryland Law pertaining to medical records is provided for general information purposes.

At the discretion of the instructor this portion of the lesson plan may be presented in its entirety or its contents can be highlighted as determined by the instructor.

✓ HG § 4-302 et al. in general provides that: → a "health care provider:" ★ keep the medical records of a patient or recipient of mental health services confidential; ★ disclose those records only as provided within the law; • re-disclosure by person to whom records are released not legal unless authorized by the patient; ★ conditions upon which medical records can be released to a third party: • valid authorization; • compulsory process: ▪ subpoena/summons/warrant/court order; ★ requirement to provide a copy of an individual's medical record to a party of interest within a reasonable amount of time (up to 21 days): • upon written request; ▪ conditions upon which a mental health provider can deny a request that relates to a psychiatric or psychological problem; • may not refuse a copy of the medical record for failure to pay for health care services rendered; ★ receive payment for copy of medical record; ★ requirement to establish procedures to add to/correct a patient's medical record; ★ conditions under which a health care provider may disclose medical records to a third party without authorization of the person of interest: • seeking payment for medical services that have been provided; • legal counsel; • insurers; • to others as enumerated in § 4-305; ★ disclosures without authorization for investigative purposes - § 4-306 (7): • subpoena/summons/warrant/court order;	(PPT SLIDE # 26)

✓ **HG § 4-303. Disclosure upon authorization of person in interest.** **(a) *In general:*** **...health care provider shall disclose medical record on authorization of person in interest in accordance with this section...** **(1) BE IN WRITING/DATED/SIGNED BY PERSON IN INTEREST;** **(2) state name of health care provider;** **(3) identify to whom information is to be disclosed;** **(4) state period of time that authorization is valid – may not exceed 1 year:** **(i) in cases of criminal justice referrals:** **• authorization shall be valid for 30 days following final disposition;** **(5) apply only to medical record developed by health care provider unless in writing:** **(i) authorization specifies disclosure of medical record...from another provider; and** **(ii) other provider has not prohibited re-disclosure.** **(c) *Pre-authorized insurance forms:*** **...shall disclose medical record on receipt of preauthorized form...part of application for insurance.** **(d) *Authorization for release related to workers' compensation claims:*** **...shall disclose medical record on receipt of authorization for release of relevant medical information included with the claim application form filed with the Workers' Compensation Commission...**	**(PPT SLIDE # 27)**

✓ **Maryland Law [HG § 4-306] allows disclosure of medical records *WITHOUT* authorization of patient or person of interest under various circumstances/with certain conditions/limitations to include:** → **investigation/treatment in case of suspected abuse/neglect of child/adult;** → **health professional licensing and disciplinary boards;** → **health care provider or provider's insurer/legal counsel when health care provider is faced with civil action initiated by patient/recipient/person of interest;** → **medical/dental review committees defined in Health Occupations Article;** → **another health care provider as provided in HG § 19-308.2/HG § 10-807;** → **during court proceedings when person of interest has waived compulsory process;** → **grand juries/prosecution agencies/law enforcement agencies to further an investigation:** * **PURSUANT TO SUBPOENA/WARRANT/COURT ORDER:** • **for SOLE purpose of INVESTIGATING AND PROSECUTING CRIMINAL ACTIVITY:** ▪ **must have written procedures to protect confidentiality of the records;** → **Maryland Insurance Administration when conducting an investigation/examination pursuant to Title 2, Subtitle 2 of Insurance Article;** → **State/local child fatality review team established under Title 5, Subtitle 7 of this Article as necessary to carry out its official functions;** → **local domestic violence fatality review team established under Title 4, Subtitle 7 of Family Law Article as necessary to carry out its official functions;** ✓ **Health care provider to insert in patient's medical file:** → **written request for disclosure;** → **written confirmation of oral request that justifies disclosure;** → **documentation of disclosure;**	**(PPT SLIDE # 28)**

✶ **HG § 4-307 deals with disclosure of MENTAL HEALTH records:** • conditions under which a medical record developed in connection with the provision of mental health services disclosed without the authorization of a person in interest; • status of/disclosure of "personal notes" of a mental health provider; • status of/disclosure of psychological tests as part of a medical record; • status of/disclosure of mental health medical records relating to obtaining or continuing employment; • other conditions for disclosure; • requirement to document disclosure and to maintain documentation in the medical record of the recipient of the mental health services;	**(PPT SLIDE # 29)**
→ **HG § 4-309 (e) FRAUDULENT OBTAINING OF RECORDS; WRONGFUL DISCLOSURE OF RECORDS:** ► **A health care provider or any person, including an officer or employee of a governmental unit who:** ✶ **KNOWINGLY/ WILLFULLY REQUESTS/OBTAINS A MEDICAL RECORD UNDER FALSE PRETENSES OR THROUGH DECEPTION; or** ✶ **KNOWINGLY/ WILLFULLY DISLOSES A MEDICAL RECORD in violation of this Subtitle is guilty of a *MISDEMEANOR*:** ✶ **This subsection does NOT apply to an officer or employee of governmental unit that is conducting a CRIMINAL investigation.**	**(PPT SLIDE # 30)**

PUBLIC/GOVERNMENT DOCUMENTS/RECORDS:

- ✓ **virtually EVERY MAJOR CHANGE IN LIFE is recorded somewhere in a government document:**
  - → **birth certificate:**
    - ► **parents' name;** ► **social security number issued;**
  - → **school enrollment:**
    - ► **personal identifiers;**
    - ► **medical/immunization record;**
  - → **driver's license:**
    - ► **magnetic strip with personal identifying information;**
  - → **work permit;**
  - → **school/academic record;**
  - → **marriage license/divorce records;**
  - → **house/property bought/sold;**
  - → **vehicle purchased/registered with State;**
  - → **tax payments:**
    - ► **income;** ► **property tax;**
  - → **professional licenses;**
  - → **death certificate;**
- ✓ **SG § 10-611 (g) defines "public record" as "the original or any copy of any documentary material that is made or received by a unit or instrumentality of State government or political subdivision in connection with the transaction of public business and is in any form:"**
  - ► **does NOT include digital photographic or signature of individual recorded by Motor Vehicle Administration;**
- ✓ **many "public" records/documents contain PERSONAL IDENTIFYING INFORMATION;**
- ✓ **some public records readily available to self/others and may even be posted online:**
  - ► **some require sufficient identification before review, e.g. birth records;**
  - ► **others do NOT require identification, e.g. property records or court records;**
- ✓ **various public records are routinely consulted/examined by:**
  - ► **employers;**
  - ► **insurance companies/financial institutions;**
  - ► **attorneys;**
  - ► **law enforcement;**
- ✓ **various requests to view public records/documents may/may not be subject to public information laws depending on the type of record;**

(PPT SLIDES # 31-42)

Instructor Note:

Public records/documents are a source of personal identifying information that can be compromised by individuals intent on identity theft.

Information regarding the availability of/access to various personal identifying information in public records is also provided in this lesson plan as a potential source of information that can be used during various types of criminal investigations.

✓ **EXAMPLES - INFORMATION THAT MAY BE CONTAINED IN PUBLIC RECORDS/DOCUMENTS:** → **BIRTH RECORD:** ★ NAME OF CHILD; ★ NAME OF PARENTS; ★ DATE AND TIME OF BIRTH; ★ CITY OF BIRTH – NAME OF HOSPITAL; ★ ATTENDING PHYSICIAN'S NAME; → **STUDENT RECORD:** ★ NAME/DATE OF BIRTH/HOME ADDRESS/HOME TELEPHONE NUMBER; ★ BIOGRAPHICAL INFORMATION; ★ FAMILY INFORMATION; ★ PHYSIOLOGY; ★ RELIGION; ★ ACADEMIC ACHIEVEMENT; ★ PHYSICAL/MENTAL ABILITY; → **MOTOR VEHICLE RECORD:** ★ PERSONAL IDENTIFYING INFORMATION; ★ PHYSICAL DESCRIPTION; ★ NOTATIONS REGARDING PHYSICAL/MENTAL CONDITIONS; ★ ISSUED DRIVER'S LICENSE NUMBER; ★ PHOTOGRAPH; ★ CONVICTIONS FOR VIOLATIONS; ★ TRAFFIC ACCIDENT HISTORY;	**(PPT SLIDE # 33)**
✓ **access to public records [in Maryland] is controlled under:** **State Government Article** **Title 10 - Governmental Procedures** **Subtitle 6 – Records** **Part III – Access to Public records** **parts of which state:** **→ SG § 10-611. Definitions:** **(c) "Custodian" means:** **(1) *official* custodian; or** **(2) any other authorized individual who has physical custody/control of a public record;**	**(PPT SLIDES # 34-42)**

(d) ***Official*** custodian – ***Official*** custodian means officer/employee of State or of political subdivision who, whether or not officer/employee has physical custody and control of public record, is responsible for keeping the public record.

(f) Personal information:

(1) Except as provided in this Part III, "personal information" means:

► information that identifies an individual including an individual's:

* address;
* driver's license number;
* any other identification number;
* medical or disability information;
* name;
* Social Security number;
* photograph/computer generated image;
* telephone number;

✓ SG § 10-613 – Inspection of Public records:

(a) In general:

(1) ...a custodian shall permit person/government unit to inspect any public record at any reasonable time.

(2) inspection/copying of public record may be denied only to extent provided under the subtitle;

(b) Rules or regulations:

To protect public records and to prevent unnecessary interference with official business each official custodian shall adopt reasonable rules/regulations that...govern timely production and inspection of a public record.

(c) Designation of specific types of public records:

Each official custodian shall consider whether to:

(1) designate specific types of public records of government unit that are to be made available to any applicant ***immediately*** upon request; and
(2) maintain current list of types of public records that have been designated as available to any applicant ***immediately*** upon request.

Instructor Note:

See definition of public record on page 24 of lesson plan.

✓ SG § 10-616. Required DENIALS. Specific RECORDS. → Unless otherwise provided by law custodian (of records) shall deny inspection of public RECORD: ★ Adoption records; ★ Welfare records; ★ Letters of Reference; ★ Circulation records/other item/collection/grouping of information about an individual: ■ e.g. library circulation/use of services records; ★ Gifts of library/archival/museum materials as limited by donor; ★ Retirement records; ★ Police records - criminal charging documents prior to service/accident reports/traffic citations; ★ certain personnel records; ★ Hospital records; ★ Student records; ★ RBC [risk based capital] records; ★ Maryland Transportation Authority records; ★ Higher education investment contracts; ★ Images from automated monitoring systems; ★ Motor Vehicle Administration records containing personal information: ► TR § 12-111 & TR § 12-112; ★ Records pertaining to arrest warrants; ★ Maryland Transit Administration records; ★ Department of Natural Resources' records containing personal information; ★ Application for renewable energy credit certification or claim for credits; ★ Surveillance images as contained in CR § 10 -112; ✓ SG § 10-617. Required DENIALS. Specific INFORMATION. → Unless otherwise provided by law custodian [of records] shall deny inspection of part of public record as provided in this section: ★ Medical and psychological information; ★ Sociological information; ★ Commercial information; ★ Financial information [does not apply to salary of public employee]; ★ Information systems [security of]; ★ Licensing records; ★ Suspected collusive or anticompetitive activity; ★ Notary publics; ★ License application containing Social Security Number [e.g. marriage license]; ★ Public record containing personal information; ★ Senior citizens activities centers;	(PPT SLIDE # 38) Instructor Note: Refer student to SG § 10-616 and 10-617 for a complete list of public records to which access can be denied. (PPT SLIDE # 39)

✓ **SG § 10-624. PERSONAL records:**

(a) "Personal record" defined:

In this section "personal record" means public record that names or with reasonable certainty otherwise identifies individual by identifying factor such as:

(1) address;
(2) description;
(3) finger or voice print;
(4) number;
(5) picture.

(b) Requirement of need:

(1) Personal records may NOT be created unless need for information has been clearly established by unit collecting records.

(PPT SLIDE # 40)

✓ **SG § 10-626. Unlawful disclosure of PERSONAL records.**

(a) A person including officer/employee of governmental unit is liable to individual for actual damages that the court considers appropriate if court finds by clear/convincing evidence that:

(1) (i) person willfully and knowingly permits inspection/use of public record in violation of this subtitle; and

(ii) public record names/with reasonable certainty otherwise identifies individual by identifying factor such as:

1. **address;**
2. **description;**
3. **finger or voice print;**
4. **number; or**
5. **picture; or**

(2) person willfully and knowingly obtains/discloses/uses personal information in violation SG §10-616 (p) [Motor Vehicle Administration records containing personal information] of this subtitle.

(PPT SLIDE # 41)

✓ **SG § 10-627. Prohibited acts; CRIMINAL penalties:** **(a) Prohibited acts:** **A person may not:** **(1) willfully or knowingly violate any provision of this subtitle;** **(3) by false pretenses/bribery/theft gain access to/obtain copy of personal record whose disclosure to person is prohibited by this subtitle;** **(b) Criminal penalties:** **A person who violates any provision of this section is guilty of:** **→ MISDEMEANOR;** **► on conviction is subject to a fine not exceeding $1,000.**	**(PPT SLIDE # 42)**

HOW IS INFORMATION STOLEN/COMPROMISED:

✓ **personal identifying information can be stolen/compromised in a variety of ways including, but not limited to when/during:**

- → **wallets/purses containing items with personal information are lost/stolen;**
- → **mail containing personal information is stolen;**
- → **trash/recyclables are rummaged through:**
  - ► **dumpster diving;**
- → **individuals may pose as persons legally authorized to obtain a person's credit report such as a landlord, employer or business;**
- → **individuals may collude with/bribe employees of businesses, government agencies or service organizations to obtain personal information;**
- → **employees of businesses, government agencies or service organizations may themselves steal and use the information;**
- → **personal information is compromised during the commission of another crime such as a robbery or a residential burglary in which personal records are taken or a home computer containing personal information is taken;**
- → **home and business computers are hacked into and customer and employee databases are stolen;**
- → **personal information is stolen through "e"mail or by phone by persons saying that they represent a legitimate company and claim there is a problem with an existing account:**
  - ► **"phishing" on line;**
  - ► **"vishing" by telephone;**
- → **false or counterfeit IDs are obtained from the Internet or other sources;**
- → **counterfeit documents such as birth certificates, visas, passports, etc. are purchased and used;**
- → **PINs/account numbers/user IDs are compromised during a legitimate transaction and then fraudulently used:**
  - ► **shoulder surfing;**
- → **Internet scams in which Internet users are tricked into providing personal information or user IDs/PINs;**
- → **a *legitimate* business transaction by an employee using a skimming device or encoder or when using an ATM machine:**
  - ► **"skimming";**
- → **data breaches occur at a government agency/school/medical facility, etc.**

(PPT SLIDES # 43-46)

TRAINING OBJECTIVE:

Identify several examples of the crime of identity theft/fraud to include, at a minimum, the theft/fraudulent use of:

- existing credit/debit cards/financial accounts;
- other financial records/personal financial information to obtain credit or other financial assistance;
- personal information to obtain various services such as medical treatment, government or social services, educational assistance, etc; and
- personal information to obtain government identity cards, licenses or other official documents.

EXAMPLE - IDENTITY THEFT - DIGITAL COPIERS:

- ✓ since 2005 hard drive installations in midsize to large digital photo copiers have become routine;
- ✓ digital copiers are commonly found in offices and businesses including pay per copy businesses, libraries, post offices, etc.
- ✓ the hard drive stores an image of any document that has been scanned or copied;
- ✓ the unencrypted data remains until the hard drive is full:
  - ► when the hard drive becomes full it overwrites old files with newer ones;
- ✓ many photocopiers use a modem and are connected to an office network;
- ✓ disposal of photocopier with personal information stored on the hard drive exposes individual's personal information to theft/fraudulent use:
  - ► no guarantee that pay per copy businesses use "disk scrubbing" software ***prior*** to disposing of used copiers;
  - ► no guarantee that pay per copy businesses use encryption software to prevent data from being stored;
- ✓ hard drives can be "reclaimed" by identity theft suspects ***after*** a copier has been disposed of for recycling purposes;
- ✓ Maryland Law - Personal Information Protection Act (PIPA) [CL § 14 – 3501 et al.] requires businesses that maintain personal information to protect that information and DISPOSE OF IT IN A MANNER THAT RENDERS IT UNREADABLE:
  - ► applies to both paper records as well as records maintained on computers or other devices with hard drives;
- ✓ improperly disposing of an individual's personal information could be considered as a violation of Maryland's PIPA;
- ✓ in the event of a security breach, notice must be given to the consumer, in writing, as soon as reasonably practicable following an investigation or by telephone to the most recent telephone number;
- ✓ the business is also required by Maryland Law to notify the Office of the Maryland Attorney General;

(PPT SLIDES # 47-48)

Instructor Note:

Given the commonplace use of digital photocopiers, especially in pay per copy businesses information concerning the theft of personal identifying information from such devices is presented for general information.

For more information about digital copiers as identity theft threat refer to Office of Maryland Attorney General website: www.oag.state.md.us

E-COMMERCE (ELECTRONIC/ONLINE SHOPPING):

✓ a 2008 survey by the Pew Organization revealed that:

→ 74% of adult Americans are Internet users;
→ 93% of adult internet users have conducted some type of financial/commercial transaction over the Internet:
► 66% of "on-line" Americans have purchased a product online:
► 64% have made some type of travel reservation;
► 39% bank online;
► 24% used classified ads on such sites as Craig's list;
► 26% have participated in an online auction;
► 17% have paid to access digital content;
► 11% have purchased/sold stocks online;

✓ prevailing attitudes of e-commerce shoppers:
→ 78% of users agreed that it is convenient;
→ 68% of users agreed that it saves time;
→ 75% of users agreed that they do not like giving their credit card number or personal information online;

✓ victims provide personal identifying information about self during E-COMMERCE transactions:
✶ name;
✶ address;
✶ credit/debit card information;

✓ many fraudulent websites appear to be legitimate sites:
→ may request user to update personal identifying information:
✶ "phishing;"

✓ once fraud/theft is discovered the victim is faced with 3 challenges when reporting/following through on prosecution:
→ because of remote nature of Internet:
► difficulty in locating/identifying suspect:
✶ may operate in other countries;
✶ suspects develop new "tricks" to stay ahead of law enforcement;
► determining jurisdiction in which to prosecute suspect;
► obtaining restitution;

(PPT SLIDES # 49 - 50)

Instructor Note:

Because of the growing amount of e-commerce, i.e. business transactions conducted over the Internet, identity theft via ***unsecured*** websites is increasing. The information presented in this section is provided to alert officers to their susceptibility to such crimes and as crime prevention information to be shared with the public .

The data in this section was taken from a Pew Internet Survey entitled Online Shopping – 2008 available at: www.pewinternet.org

Information Resource:

Privacy Rights Clearinghouse – Fact Sheet: Online Privacy – Using the Internet Safely www.privacyrights.org

✓ **users/consumers need to take responsibility for own risk management strategy:** → **use only <u>CREDIT</u> card for online financial transactions:** ► **debit cards normally do <u>not</u> provide protection from fraud:** ✶ **access to checking account may result in entire checking account balance being lost;** ✶ **use of <u>CREDIT</u> card allows victim to dispute unauthorized charges;** ✓ **reputable businesses normally use <u>SECURED</u> websites with up to date security certificates:** → **web address with letter "s" attached to *<u>http</u>* in address bar:** ✶ **indicates financial information will be encrypted during transmission;** ✓ **businesses <u>legitimately</u> buy/sell/share user information with/to each other:** → **DATA MINING by way of "Web bugs";** ✓ **reputable online auction sites issue fraud alerts posted by online;**	

HOW **the information is USED:**

- ✓ **identity theft is often part of a larger criminal scheme and involves other statutory prohibitions against credit card fraud, computer fraud, mail fraud or wire fraud;**
- ✓ **there are TWO MAIN MOTIVES FOR IDENTITY THEFT:**
  - ► **FINANCIAL GAIN;**
  - ► **CONCEALMENT OF:**
    - ✶ **TRUE IDENTITY:**
      - **PERSONAL HISTORY;**
      - **PAST CRIME/CRIMINAL HISTORY;**
- ✓ **while there are countless ways a victim's personal identifying information can be used, the following are the TYPICAL ILLEGITIMATE uses for this information:**
  - → **open a NEW CREDIT CARD account;**
  - → **open a landline or CELLPHONE account;**
  - → **open a UTILITIES account to obtain services;**
  - → **open a CHECKING account by which bad checks are written;**
  - → **create counterfeit checks/credit/debit cards using another individual's identity;**
  - → **file for bankruptcy under the victim's name to avoid paying their own debts or to avoid eviction;**
  - → **take over existing insurance policies or make false claims with the insurance company;**
  - → **take out loans such as auto loans, personal loans or mortgages;**
  - → **submit fraudulent tax returns in order to collect refunds;**
  - → **submit applications for social security numbers;**
  - → **apply for and receive services from various government agencies or other organizations such as medical treatment;**
  - → **use the victim's name/information for identification when stopped by law enforcement or charged with a crime;**
  - → **use stolen IDs to obtain credit/access to existing accounts/services;**

(PPT SLIDES # 51-52)

TRAINING OBJECTIVE:

Identify several different ways in which personal information including financial information may be stolen/compromised, to include at a minimum:

- the use of home computers;
- discarded/stolen mail;
- discarded personal and/or financial records;
- theft/compromise during the *legitimate* use of information by victim during a third party transaction.

SCOPE OF IDENTITY THEFT/FRAUD:

(PPT SLIDES # 53-57)

✓ data sources regarding identity theft/fraud vary in quality concerning the information that they provide:

→ provide conflicting/different estimates concerning the extent and cost of identity theft:

► tendency of businesses to exaggerate the threat of identity theft in order to sell products tailored to prevent identity theft or to combat its effects:

- computer software;
- insurance products;

✓ there are several reliable identity theft data sources:

→ Federal Trade Commission:
► assigned the responsibility of collecting data as a result of the Identity Theft Act of 1998;

→ U.S. General Accounting Office;

→ Social Security Administration;

→ Postal Service;

→ Department of Homeland Security;

→ Federal Bureau of Investigation;

→ United States Secret Service;

→ various credit reporting agencies;

→ Javelin Strategy and Research:
► private research firm focusing on financial issues;

Instructor Notes:

The Federal Trade Commission (FTC) is the main clearinghouse for information concerning identity theft/fraud. www.ftc.gov

There are a variety of sources that provide statistical data regarding identity theft/fraud. Several different sources are used and identified throughout this lesson plan.

Instructors should periodically refer to the various listed sites to update the statistical information contained in this lesson plan as needed.

✓ **a national crime victimization survey conducted by the U.S. Department of Justice entitled *"Victims of Identity Theft, 2008"* highlighted the following:** **→ an estimated 11.7 million persons, representing 5% of all persons age 16 or older in the United States, experienced at least one type of identity theft in a 2-year period;** **→ the unauthorized misuse/attempted misuse of a credit card was the MOST PREVALENT type of identity theft:** **► reported by 10.1 million persons age 16 or older:** **• 6.2 million experienced the fraudulent use of an *EXISTING* credit card account;** **→ 4.4 million persons reported the fraudulent use of bank accounts;** **→ 1.7 million victims reported the fraudulent misuse of their personal information to open some type of *NEW* account;** **→ 39% of the identity theft victims believed they knew how their identifying information was obtained:** **► 30% believed the theft occurred while making a purchase;** **→ 618,900 victims reported the misuse of their personal identifying information to commit other crimes such as:** **► fraudulently obtaining medical care;** **► fraudulently obtaining government benefits/services;** **► providing false information to law enforcement during a crime or traffic stop;** **→ 1.8 million persons experienced *MULTIPLE* types of identity theft usually involving:** **► the unauthorized use of a combination of *EXISTING* accounts such as:** **• credit cards;** **• checking accounts;** **• savings accounts;** **• telephone/on-line accounts;**	**Instructor Note:** **The special report entitled "Victims of Identity Theft, 2008" is available at:** **www.ncjrs.gov** **www.ojp.usdoj.gov** **The report is based on data collected from persons who reported that they had experienced one or more attempted or successful incidents of identity theft during the two years preceding their interview with the U.S. Department of Justice researchers.** **Some of the statistical information presented in this section has been taken from "Identity Theft Consumer Complaint Data – January – December 2009 published by the Federal Trade Commission and available at www.ftc.gov** **NOTE:** **Consumer identity theft complaints filed with the FTC may be coded under multiple theft types.**

→ **IN 2008, ONLY 17% OF IDENTITY THEFT VICTIMS REPORTED THE INCIDENT TO A LAW ENFORCEMENT AGENCY:**

► 80% of identity theft victims who did not report an incident to the police offered a variety of reasons for lack of contact:

- the most common was that the victim handled the theft in different way such as reporting it to a credit card company/bank/other organization;

► **19% believed that the police could NOT help them;**

✓ the Federal Trade Commission reported in its annual publication entitled "Identity Theft Consumer Complaint Data for 2009" the following:

→ there were 278,078 ***self-reported*** consumer complaints involving identity theft filed with the Federal Trade Commission - Consumer Sentinel Network from January 1 – December 31, 2009:

✶ **5,232 identity theft consumer complaints from Maryland;**

→ **Maryland ranked 11th nationwide in the number of consumer complaints per 100,000 persons:**

✶ **91.8 complaints per 100.000 persons;**

✓ fraud complaints were categorized as follows:

TYPE OF FRAUD	NATIONWIDE	MARYLAND
▪ CREDIT CARD	17%	22%
▪ GOVERNMENT DOCUMENTS/BENEFITS	16%	12%
▪ PHONE/UTILITIES	15%	13%
▪ EMPLOYMENT RELATED	13%	8%
▪ BANK	10%	14%
▪ LOAN	4%	4%
▪ OTHER IDENTITY	23%	24%
▪ ATTEMPTED IDENTITY	6%	7%

(PPT SLIDE # 56)

Instructor Note:

The percentage figures indicate the percent of ***self-reported*** complaints filed with the FTC from Maryland residents in 2009:

- a total of 5,232 complaints were filed.

Total exceeds 100% due to report of multiple crimes.

✓ **the 5,232 identity fraud complaints from Maryland filed with the FTC were further broken down as follows:**

- **CREDIT CARD – 22%:**
  - ***NEW*** **accounts – 11.8%**
  - ***EXISTING*** **accounts – 10.3%**
- **GOVERNMENT DOCUMENTS/BENEFITS – 12%:**
  - **TAX or WAGE RELATED – 9.2%**
  - **BENEFITS APPLIED FOR/RECEIVED – 1.5%**
  - **OTHER DOCUMENTS ISSUED/FORGED – 0.9%**
  - **DRIVER'S LICENSE ISSUED/FORGED – 1.2%**
- **PHONE/UTILITIES FRAUD – 13%:**
  - **UTILITIES –** ***NEW*** **account – 5.5%**
  - **WIRELESS –** ***NEW*** **account – 5.4%**
  - **TELEPHONE –** ***NEW*** **account – 1.9%**
  - **UNAUTHORIZED CHARGES -** ***EXISTING*** **account – 0.7%**
- **EMPLOYMENT RELATED FRAUD – 8%**
- **BANK FRAUD – 14%:**
  - **ELECTRONIC FUND TRANSFER – 5.9%**
  - ***EXISTING*** **accounts – 4.4%**
  - ***NEW*** **accounts – 3.7%**
- **LOAN FRAUD – 4%:**
  - **BUSINESS/PERSONAL/STUDENT – 1.7%**
  - **AUTO LOAN/LEASE – 1.1%**
  - **REAL ESTATE LOAN – 1.3%**
- **OTHER IDENITY THEFT – 24%:**
  - **UNCERTAIN/MISCELLANEOUS – 18.2%**
  - **EVADING THE LAW – 1.2%**
  - **MEDICAL – 1.2%**
  - **INTERNET/"E" MAIL – 1.7%**
  - **APARTMENT/HOUSE/PROPERTY RENTAL – 1.3%**
  - **INSURANCE – 0.2%**
  - **CHILD SUPPORT – 0.1%**
  - **MAGAZINES – 0.2%**
  - **BANKRUPTCY – 0.1%**
  - **SECURITIES/OTHER INVESTMENTS – 0.2%**
- **ATTEMPTED IDENTITY THEFT – 7%;**

ECONOMIC IMPACT OF IDENTITY THEFT:

(PPT SLIDES # 58-62)

- ✓ the economic impact of identity theft can be broken down into ***DIRECT*** and ***INDIRECT*** financial loss;
- ✓ in 2008, 62% of identity theft victims reported either direct or indirect financial loss associated with an identity theft during the prior 2 years:
- ✓ victims of identity theft reported a cumulative financial loss of nearly $17.3 billion during the 2 year period;
- ✓ the percentage of victims that suffered any financial loss varied by type of identity theft:
  - → credit card – 61%
  - → bank card fraud – 70%
  - → NEW account fraud – 48%
  - → personal information fraud – 24%
- ✓ 70% of victims reporting multiple types of identity theft experienced financial loss;

- ✓ DIRECT FINANCIAL LOSS:
  - → the monetary amount the offender obtained from misusing the victim's account or personal information:
    - ► the estimated value of good/services/cash obtained:
      - 59% of identity theft victims reported a ***DIRECT*** FINANCIAL LOSS totaling more than $16.6 billion:
        - ✶ an average of $2,400 per victim;
      - the number of victims experiencing a ***DIRECT*** financial loss over the two year period varied by the type of identity theft:
        - ✶ 59% credit card fraud victims:
          - ▪ average loss of $1,105;
        - ✶ 68% bank card fraud victims;
        - ✶ 42% new account fraud victims:
          - ▪ average loss of $8,110;
        - ✶ 18% personal information theft victims:
          - ▪ average loss of $2,289;

Instructor Note:

Data regarding the economic impact of identity theft was taken from *"Victims of Identity Theft, 2008"* published by the Department of Justice, Bureau of Justice Statistics. www.ojp.usdoj.gov

The data presented in this report was based on information taken from crime victims, age 16 years and older, over a two year period between 2006-2008. Over 56,000 victims completed the survey.

Instructors should periodically update the information in this section.

(PPT SLIDES # 60-61)

• 69% of victims who experienced multiple types of identity theft/fraud reported an average DIRECT LOSS of $4,680; • approximately 16% of all identity theft victims reported DIRECT *OUT-OF-POCKET* personal losses totaling over $4.1 billion over the two year period: * average of $2,228 per victim; ✓ INDIRECT FINANCIAL LOSS: → any other costs accrued because of identity theft: ► legal fees; ► bounced checks; ► miscellaneous expenses to the victim; → 11% of all identity theft victims reported *INDIRECT* losses which totaled $1.04 billion: * average reported INDIRECT LOSS of $788; • victims who experienced the fraudulent misuse of their personal information reported the largest average INDIRECT LOSS of $3,955; → victims of NEW account fraud averaged an INDIRECT financial loss of $7,250; ✓ 42% identity theft victims reported that they spent a day or less to resolve financial or credit problems associated with the theft: → 27% spent MORE THAN A MONTH from the discovery of the theft trying to clear up problems;	(PPT SLIDE# 62)

✓ *2010 Identity Fraud Survey Report* – Javelin Strategy and Research:

→ the number of identity fraud victims in the United States increased to 11.1 million adults in 2009 – a 12% increase
  ► 4% of the United States population;

→ the total annual fraud amount increased to a projected $54 billion – a 12.5% increase:
  ► fraud costs per victim were down;

→ the average fraud resolution time dropped to 21 hours – a 30% decrease;

→ consumer out-of-pocket costs were $373 in 2009:
  ► unreimbursed losses;
  ► legal fees; etc.

→ NEARLY 50% OF THE VICTIMS NOW FILE POLICE REPORTS:
  ► arrest rates doubled over 2008 rates;
  ► prosecution rates tripled over 2008 rates;

→ identity information most likely to be compromised are:
  ► FULL NAME – 63%;
  ► PHYSICAL ADDRESS – 37%;
  ► SOCIAL SECURITY NUMBER – 32%;

→ while still a relatively small amount (4%) of the total of identity theft, HEALTH INSURANCE INFORMATION is being increasingly targeted for fraud;

→ the number of NEW credit card accounts opened using stolen information increased to 39% of all identity fraud victims:
  ► a 33% from 2008;
  ► NEW on-line accounts opened fraudulently increased more than 50%:
    • new e-mail payment accounts increased 12%;

→ fraudsters targeted EXISTING CREDIT CARDS:
  ► 75% of existing card fraud involved credit cards;
  ► existing debit card fraud decreased 2% to 33%;

→ 29% of fraud victims reported that NEW mobile phone accounts had been opened;

→ 18-24 year olds are the slowest to detect fraud and as a result are fraud victims for a longer period of time:
  ► least likely to monitor accounts regularly;
  ► most likely to install anti-malware on their computer when they discover fraud;

Instructor Note:

Javelin Strategy and Research conducts syndicated research for the business community in the area of identity theft.

A summary of its 2010 Identity Fraud Survey Report is included in this lesson plan to provide a "current" picture of identity fraud.

The data presented is a summary of the latest report summarized in a press release from Javelin Strategy and Research, February 2010.

The 2009 telephone survey conducted by Javelin included more than 5,000 victims of identity fraud.

PORTRAIT OF A VICTIM of Identity Theft:

(PPT SLIDES # 66-69)

✓ virtually ANYONE MAY BECOME A VICTIM OF IDENTITY THEFT:
- ► *NOT* just the affluent:
- ► ANYONE WITH GOOD CREDIT;

✓ the Federal Trade Commission has described the characteristics of the "average" identity theft victim:

→ spans ALL AGE CATEGORIES:
- ► average victim age is 42:

→ victimization rates may be correlated to Internet use:
- ► may account for the large number of victims under 40 years:
  - 44% of identity theft victims;
- ► seniors are less likely to be victimized by identity theft by computer but more susceptible to telephone scams;

→ most victims live in a metropolitan area but an increasing number of victims live in rural areas;

→ typically do not notice the crime for 14+ months;

→ a greater percentage of identity theft victims live in higher income households – more than $75,000 per year than in lower income households;

→ similar percentage of men and women experience identity theft;

→ minority victims may suffer from non-credit card identity theft, especially theft of telephone and other utility services and check fraud;

✓ approximately 4.5 million, or 40% of identity theft victims, had some idea as to how the identity theft occurred:

→ 30% believed their identity was stolen during a purchase or other transaction;

→ 20% believed the information was lost or stolen from a wallet or checkbook;

→ 14% thought the information was stolen from personnel or other files at their office;

→ 11% thought the information was stolen from the location where it was stored;

→ 8% believed that family or friends had stolen their information;

→ 17% believed that their information had been stolen by other means such as:
- ► their computer had been hacked;
- ► their personal information had been compromised on the internet;
- ► it had been stolen from their mailbox or removed from their garbage/recyclables;

Instructor Note:

The Federal Trade Commission has provided a general portrait of the "average" identity theft victim. It is presented in this lesson plan for informational purposes.

✓ approximately 40% of identity theft victims had some idea as to how the identity theft occurred: → 50% of victims who had multiple types of identity theft during the same incident knew how the theft occurred; ✓ 40% of identity theft victims who had personal information used fraudulently AND knew how their information was obtained believed FAMILY/FRIENDS WERE RESPONSIBLE; ✓ CHILDEREN as identity theft victims: → have a social security number: ► used to open accounts/establish credit: ✶ credit limit reached: ■ defaults on account leaving child victim; ► SSN stolen from medical records, school files or other legitimate government/service agencies; ✓ DECEASED as identity theft victims: → obituaries read: ► social security number stolen; ► fraudulent SSN obtained using deceased identity; **VICTIM RESPONSE TO IDENTITY THEFT:** ✓ the majority of identity theft victims notified a financial institution/organization or government entity to report the theft and misuse or attempted misuse of an account or personal information: → 68% contacted a credit card company; → about 15% contacted a credit bureau; → 7% contacted a credit monitoring service; → 1% contacted the Federal Trade Commission; → 3% contacted a government consumer affairs agency or other consumer protection organization; → 4% contacted an agency that issues identity documentation such as the Social Security Administration or the Motor Vehicle Administration; → ONLY 17% CONTACTED A LAW ENFORCEMENT AGENCY TO REPORT THE INCIDENT; ✓ of the 17% of victims who contacted a law enforcement agency they breakdown as follows: → 28% were victims of NEW account fraud; → 26% were victims of MULTIPLE IDENTITY THEFT; → 26% were victims of PERSONAL INFORMATION MISUSE; → 13% were victims of UNAUTHORIZED USE OF EXISTING ACCOUNTS;	(PPT SLIDES # 70-72)

✓ 83% of victims who did not report the incident to police offered a variety of reasons for the lack of contact:
- → 48% handled the complaint a different way such as reporting the theft to their credit card company, etc.
- → 22% did not report the incident because they did not suffer any monetary loss;
- → 19% did not believe that the police could help them;
- → 15% did not know that they could report the incident to the police;
- → 7% chose not to report the incident because they were afraid, embarrassed or thought reporting the incident would inconvenience them;
- → less than 1% did not report the incident because it involved a family member or friend;

VICTIM DISTRESS/OTHER NON-FINANCIAL IMPACT:

(PPT SLIDES # 63-65)

✓ as with other incidents of crime victim stress to identity crime varied:
- → 11% did NOT suffer from any stress;
- → 34% found the incident MILDLY DISTRESSING;
- → 33% found it MODERATELY DISTRESSING;
- → 20% found it SEVERELY DISTRESSING;

✓ the level of emotional distress on victims of identity theft varied by type of incident:

TYPE OF IDENTITY THEFT	MODERATE/SEVERE STRESS
TOTAL IDENTITY	53%
CREDIT CARD	42%
BANK ACCOUNT	59%
NEW ACCOUNT	58%
PERSONAL INFORMATION	67%
MULTIPLE TYPES	60%
VIOLENT CRIME – ALL TYPES	55%

✓ victims who experienced theft of PERSONAL INFORMATION experienced a direct negative impact on work/school and family relationships compared to those who were victims of the unauthorized use of credit card;

✓ **victims who spent more time resolving financial and credit problems resulting from identity theft were more likely to experience severe distress than victims who cleared up the problem more quickly:** → **40% of victims who spent more than 6 months resolving identity theft problems reported that identity theft was severely distressing;** → **less than 15% of victims who spent a day or less resolving problems found the incident severely distressing;** ✓ **identity theft victims may experience long-term and well-documented pain and suffering such as:** → **harassment from debt collectors;** → **banking problems;** → **loan rejection;** → **utility cutoffs;** → **employment denial because of credit problems;** ✓ **a significant feature of identity theft is the offender's REPEATED VICTIMIZATION of the individual:** → **BY REPEATEDLY USING A STOLEN CREDIT CARD, TAKING OVER AN ACCOUNT OR USING STOLEN PERSONAL INFORMATION TO OPEN NEW ACCOUNTS:** ► **repeated use of victim's identity may cause serious disruption to his/her life and emotional damage;** ✓ **prior to the mid-1990's law enforcement did not generally regard those whose identity had been stolen as "true" victims of crime since the credit card companies absorbed most, if not all, of the financial loss:** → **victims rarely reported the loss or theft to police since they believed the credit card company would cover the loss;** ✓ **currently, credit card companies and other financial institutions require that victims report identity theft incidents to law enforcement as part of an "identity theft affidavit;"** ✓ **the estimated cost to law enforcement ranges from $15,000 to $25,000 to investigate each case of identity theft;**	

RECOMMENDED VICTIM RESPONSE TO IDENTITY THEFT:

✓ victim must ACT QUICKLY and assertively to minimize the damage to his/her credit history;

✓ BEGIN AND MAINTAIN A LOG OF:
- ► ALL CONVERSATIONS/CONTACTS WITH:
  - ✶ LAW ENFORCEMENT AUTHORITIES;
  - ✶ FINANCIAL INSTITUTIONS:
    - DATES;
    - NAMES;
    - PHONE NUMBERS;
    - TOPICS OF CONVERSATION;
    - TIME SPENT;
    - EXPENSES INCURRED;
- ► CONFIRM CONVERSATIONS IN WRITING:
  - ✶ SEND ALL CORRESPONDENCE BY CERTIFIED MAIL – RETURN RECEIPT REQUESTED;
- ► MAKE/RETAIN COPIES OF ALL CORRESPONDENCE AND DOCUMENTS;

✓ IMMEDIATELY PLACE FRAUD ALERT ON CREDIT REPORT:
- ► EXPERIAN – (888) 397-3742 www.experian.com
- ► EQUIFAX – (888) 766-0008 www.equifax.com
- ► TRANSUNION – (800) 680-7289 www.transunion.com
  - ✶ notification of one credit bureau results in notification of all three;
- ► request to add a victim's statement to your credit report such as:
  "My ID has been used to apply for credit fraudulently. Contact me at [victim telephone number] to verify all applications."
- ► fraud alerts are in place for 90 days:
  - ✶ renewable for a second 90 day period;
  - ✶ a victim of identity theft WITH A POLICE REPORT can request for an EXTENDED FRAUD ALERT:
    - for 7 years;

✓ CONTACT ONE OF THE CREDIT REPORTING AGENCIES:

- ► REQUEST a copy of CREDIT REPORT:
  - ✶ free credit report through the federal Fair Credit Reporting Act:
    - 1 (877) 322-8228
    - www.annualcreditreport.com
  - ✶ identity theft victims who place a fraud alert are entitled to a free credit report once an alert has been placed on their credit;

Instructor Note:

The information presented in this section is provided so that responding officers are able to provide relevant information to a victim of identity theft regarding their response to the identity theft crime.

In cases of identity theft the victim has a responsibility to take certain actions on his/her own behalf to protect his/herself from or limit financial liability.

Officers can direct victims to visit a variety of websites for pertinent information including the Office of the Maryland Attorney General at www.oag.state.md.us
or
410 - 576 -6300
1 (888) 743-0023

Additionally, this information is presented in this detailed format for the use of officers in the event that they or their family members become a victim of identity theft.

Responding officers should be encouraged to provide an identity theft victim with a copy of the page entitled Victim Assistance Information which is part of the Uniform Identity Theft Report or a reasonable facsimile provided by the law enforcement agency.

► **CAREFULLY REVIEW the credit report for any unauthorized activity:**

► **INQUIRE ABOUT THE CREDIT BUREAU'S PROCEDURES FOR INVESTIGATING AND REMOVING ERRONEOUS INFORMATION FROM REPORT:**
- ✶ **ask for sample letters to dispute fraudulent accounts on credit report;**

► **ASK FOR THE PHONE NUMBERS AND ADDRESS OF CREDIT GRANTORS WITH WHOM FRAUDULENT ACCOUNTS HAVE BEEN OPENED;**

► **request credit bureau that removes erroneous information to send an updated credit report to any business or organization that received your credit report in the last year:**
- ✶ **two years for employers;**

✓ **If the credit bureaus are not responsive contact the Maryland Division of Financial Regulation:**
- ► **410-330-6830**

✓ **MARYLAND LAW ALLOWS VICTIMS OF IDENTITY THEFT TO PLACE A "CREDIT FREEZE" ON THEIR FINANCIAL INFORMATION:**
- ► **CREDIT FREEZE blocks credit reporting agencies from sharing victim's credit report with potential creditors without the victim's express permission:**
  - ✶ **Maryland law prohibits credit reporting agencies from charging more than $5 per credit freeze:**
    - **by certified mail; or**
    - **telephone;**
- ► **each credit reporting agency has its own information requirements for filing for a CREDIT FREEZE:**
  - ✶ **websites contain that information;**
- ► **CREDIT FREEZE is available FREE to identity theft victims IF THEY SEND A COPY OF THE POLICE REPORT WITH A LETTER REQUESTING THE FREEZE;**

✓ **APPLY FOR/OBTAIN IDENTITY THEFT PASSPORT:**
- ► **CONTACT IDENTITY THEFT UNIT – OAG:**
  - ✶ **IDTheft@oag.state.md.us**
  - ✶ **410-576-6491**
- ► **IDENTITY THEFT PASSPORT may help prevent accidental arrest if an identity thief uses victim's personal identifying information during commission of a crime;**
- ► **application from OAG AND A COPY OF THE POLICE REPORT REQUIRED;**

(PPT SLIDES # 73-77)

Reference:

www.oag.state.md.us

✓ **NEW ACCOUNT FRAUD:**

→ may be discovered when reviewing credit report or upon receiving a payment/account statement from the creditor;
→ file a police report as soon as possible;
→ contact/notify all creditors with whom identity has been fraudulently used:
► by phone and in writing;
→ likely to be required to fill out a uniform fraud affidavit available from Federal Trade Commission at:
► www.consumer.gov/idtheft
→ request creditors to furnish you and local law enforcement copies of documents:
► used to open the new account:
✶ applications;
► transaction records of fraudulent transactions:
✶ may require a copy of the police report;
→ sample letters may be obtained from:
► IDTheft@oag.state.md.us

✓ **EXISTING ACCOUNT FRAUD:**

→ may be discovered when reviewing credit report or upon receiving a payment/account statement from a creditor;
→ file a police report as soon as possible;
→ contact/notify creditors holding the account *immediately* and obtain replacement cards with new account numbers:
► Federal law allows 60 days to report the fraudulent charges:
✶ if fraudulent use is reported within 60 days the credit card company cannot hold individual accountable for more than $50 worth of charges;
► notification by telephone should be followed up by written notification, preferably certified mail;
→ continue to monitor credit card statements/bills for new fraudulent activity and REPORT IT IMMEDIATELY;
→ add passwords to all accounts;

✓ **ATM cards:**

→ report theft/compromise to the bank immediately and request a fraud affidavit:
► obtain a new card/account number/password:
✶ do NOT use old password;
→ monitor account statement;

Instructor Note:

The more specific tips regarding a victim's response to any of the listed types of identity theft/fraud presented in this section of the lesson plan should be discussed with participants in the training at the discretion of the instructor.

Basic tips for a victim's response are contained in PPT SLIDES # 75-77.

→ **Federal Law affords MORE PROTECTION TO CREDIT CARD ACCOUNTS THAN ATM/DEBIT CARDS:**
- ► **fraudulent ATM/debit card use IF REPORTED:**
  - ✶ **WITHIN 2 BUSINESS DAYS:**
    - • **up to $50 liability;**
  - ✶ **WITHIN 2 – 60 DAYS:**
    - • **up to $500 liability;**
  - ✶ **if NOT REPORTED within 60 days:**
    - • **responsible for ALL unauthorized charges;**

✓ **PHONE AND UTILITY SERVICES:**

→ **contact the service provider immediately if unauthorized services have been established in victim's name:**
- ► **CANCEL the account:**
- ► **DISPUTE the charges on existing utility bill as outlined in NEW account;**

✓ **STOLEN CHECKS AND FRAUDULENT BANK ACCOUNTS:**

→ **notify bank immediately:**
- ► **obtain fraud affidavit;**
- ► **stop payment on the checks;**
- ► **close existing checking and savings accounts and open new ones;**
- ► **set a password for the new accounts;**
- ► **request bank to notify check verification service of theft;**

✓ **FRAUDULENT CHANGE OF ADDRESS:**

→ **if you believe mail has been used to commit fraud, notify the U.S. Postal Inspection Service:**
- ► **410 – 715 - 7700**

→ **find out address to which fraudulent credit cards had been sent and notify local postmaster for that address to forward all mail in YOUR name to YOUR address;**

✓ **SOCIAL SECURITY NUMBER MISUSE:**

→ **notify the Social Security Administration's Office of the Inspector General if SSN has been used to fraudulently obtain benefits:**
- ► **1 – 800 – 269 - 0271**

✓ **DRIVER'S LICENSE NUMBER MISUSE:**

→ **if driver's license number is being used as identification on bad checks contact the Motor Vehicle Administration to obtain a new driver's license number:**
- ► **1 – 800 – 950 – 1682**

✓ **FILING FOR FALSE BANKRUPTCY:** → if someone has filed for bankruptcy in victim's name victim should write to U.S. Trustee in the region where the bankruptcy was filed: ► list of U.S. Trustee Program's Regional Offices available at: ✶ www.usdoj.gov/ust → victim may have to hire a lawyer to convince bankruptcy court that the filing is fraudulent; ✓ **CRIMINAL IDENTITY THEFT:** → THE FRAUDULENT USE OF PERSONAL INFORMATION IN THE COMMISSION OF A CRIME: ► imposter uses name of other when arrested: ✶ may have arrest warrants issued using that name; → if criminal violations are wrongfully attributed to victim contact either police department or court that issued the warrant: ► file police report: ✶ request to have criminal justice databases corrected: • retain copy of police report for immediate referral until databases are cleared; ► contact State's Attorney's Office of county in which prosecution will/has occurred: ✶ www.mdsaa.org → obtain a fact sheet and additional information from: ► www.privacyrights.org ✶ 1 – 619 – 298 – 3396 → a lawyer may have to be retained to help clear the victim's name;	(PPT SLIDE # 77)

PORTRAIT OF IDENTITY CRIME SUSPECT:

(PPT SLIDES # 78-81)

✓ individuals who commit identity theft are normally categorized as being either:
- ► OPPORTUNISTIC or
- ► PROFESSIONAL (organized);

✓ individuals who engage in identity theft typically have two motives for their crime:
- ► FINANCIAL GAIN;
- ► CONCEALMENT OF TRUE IDENTITY:
  - ✶ cover up past crimes;
  - ✶ avoid capture;

✓ the most common type of opportunistic identity theft for CONCEALMENT occurs when an individual gives the name of an acquaintance/friend/family member when stopped/questioned/arrested by police;

✓ in 2009, 13% of all identity theft crimes were committed by individuals previously known to the victim including:
- ► family members;
- ► friends/acquaintances;
- ► co-workers;
- ► individuals with whom the victim has an on-going business or financial relationship;

(PPT SLIDE # 80)

✓ offenders who are OPPORTUNISTIC:

- ► take advantage of an available opportunity to steal/compromise a victim's identity:
- ► typically motivated by immediate personal need:
  - ✶ usually to solve an immediate problem:
    - ● typically a financial need:
      - ■ support a drug habit;
- ► may have legitimate access to the victim's information;
- ► generally have a low level of commitment to the crime:
  - ✶ may stop using the information after a short period of time;

  Example:

  Individual uses victim's personal information to open a new credit card:
  - ● family member/relative;
  - ● co-worker;
  - ● waiter in a restaurant;
- ► tend to act alone/individually;
- ► may graduate to PROFESSIONAL status based on their success as an opportunistic thief and long term needs;

✓ offenders who are **PROFESSIONAL:** ► may work alone or in groups: ✶ may be composed of specific ethnic or national groups or may be simply a collection of criminals of various backgrounds cooperating to obtain illegal profit by way of identity theft; ► may specialize in one type of identity theft; ► may have specialized skills/knowledge of techniques to commit particular type of identity theft; ► create their own opportunities to steal/compromise a victim's identity: ✶ seek out targets; ► carefully plan and organize their efforts to steal and use the victim's information: ✶ systematically steal identifying information; ► generally have a high level of commitment to the crime: ✶ committed to a continued use of the victim's information for an extended period of time; Example: Individuals who ***systematically*** steal personal information and fraudulently use the information as part of an on-going criminal enterprise: • gang members; • organized crime; ► tend to be geographically located far from victim's place of work or residence; ► may be local/regional/national or international in scope; ✓ identity crime is increasingly used by the PROFESSIONAL to fund criminal enterprises including: ► drug trafficking; ► gang related activities; ► terrorism;	(PPT SLIDE # 81)

FEDERAL ACTION:

- ✓ investigation of identity crimes may be conducted by a number of federal agencies including the:
  - → FBI;
  - → Secret Service; and
  - → Postal Inspection Service;
- ✓ primary jurisdiction and the lead investigative role depends upon the nature and method of theft;
- ✓ there were/are a number of federal statutes that allow for the prosecution of such crimes as:
  - ✶ the unauthorized use of a credit card;
  - ✶ the use of a false SSN to obtain a tax refund;
  - ✶ presenting false passports or immigration documents to enter the United States;
- ✓ in 1998 Congress enacted the IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT in response to the growing problem of identity theft;
- ✓ IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT OF 1998 – 18 USC § 1028 (a) (7) makes it a ***FEDERAL*** crime for anyone to:
  - → KNOWINGLY TRANSFER/POSSESS/USE:
    - ► WITHOUT LAWFUL AUTHORITY

    A MEANS OF IDENTIFICATION OF ANOTHER PERSON
    - ► WITH ANY NAME OR NUMBER THAT MAY BE USED ALONE OR IN CONJUNCTION WITH ANY OTHER INFORMATION;

    TO IDENTITY A SPECIFIC INDIVIDUAL WITH THE INTENT TO:
    - ► COMMIT/AID/ABET:
      - • ANY UNLAWFUL ACTIVITY THAT CONSTITUTES A VIOLATION OF FEDERAL LAW OR THAT CONSTITUTES A FELONY UNDER ANY APPLICABLE STATE OR LOCAL LAW.

(PPT SLIDES # 82-85)

Instructor Note:

The applicable FEDERAL laws are summarized in this lesson for informational purposes.

Given the possibility that a crime involving identity theft may be part of a larger criminal scheme which may involve violations of federal credit card, computer, mail or wire fraud statutes and extend beyond local jurisdictional borders, federal law enforcement authorities may become participants in a particular investigation.

It should be noted that while federal agencies may have authority over the investigation of a particular type of identity crime many, if not all, have established a threshold that must crossed or criteria that must be met for their involvement in a particular investigation. Local agencies are therefore responsible for the follow-up investigation in the majority of identity crime incidents.

✓ **the statute defines "means of identification" as A TYPE OF DOCUMENT INTENDED OR COMMONLY ACCEPTED FOR THE PURPOSES OF IDENTIFICATION OF INDIVIDUALS :** **→ NAME;** **→ DATE OF BIRTH;** **→ SOCIAL SECURITY NUMBER:** **► other official government identification numbers:** **• issued driver's license or identification number;** **• alien registration number;** **• government passport number;** **• employer or taxpayer identification number;** **→ UNIQUE BIOMETRIC DATA:** **► fingerprints;** **► voice prints;** **► retina or iris image;** **► other unique physical representation;** **→ UNIQUE ELECTRONIC IDENTIFYING NUMBER, ADDRESS OR ROUTING CODE:** **►credit card account numbers;** **→ TELECOMMUNICATIONS IDENTIFYING INFORMATION OR ACCESS DEVICE;** **→ ANY OTHER PIECE OF INFORMATION THAT MAY BE USED ALONE OR IN CONJUNCTION WITH OTHER INFORMATION:** **► TO IDENTIFY ANY SPECIFIC INDIVIDUAL;** ✓ **the statute also empowers the FTC to:** **► act as the national clearinghouse for information related to identity theft crimes;** **► establish a number of central resources to provide information to law enforcement agencies about identity theft crimes;** **► provide guidance to identity theft victims in order to defend themselves against the effects of this crime;** **IDENTITY THEFT PENALTY ENHANCEMENT ACT:** ✓ **enacted in 2004, establishes a mandatory 2 year minimum sentence to be served in addition to the sentence the individual receives for aggravated identity theft;**	

MARYLAND CRIMINAL LAW

CRIMINAL LAW
TITLE 8.
FRAUD AND RELATED CRIMES
SUBTITLE 3.
IDENTITY FRAUD.

§ CR 8-301. IDENTITY FRAUD.

(a) *Definitions.*

(1) In this section the following words have the meanings indicated.

(4) "PAYMENT DEVICE NUMBER" has the meaning stated in:

→ § 8-213 of this title:

(e) *Payment device number.*

...a code, account number or other means of account access, other than a check, draft or similar paper instrument:

- **that can be used to obtain money, goods, services, or anything of value, or for purpose of initiating a transfer of funds.**

(5) "PERSONAL IDENTIFYING INFORMATION" includes:

- **→ name;**
- **→ address;**
- **→ telephone number;**
- **→ driver's license number;**
- **→ Social Security number;**
- **→ place of employment;**
- **→ employee identification number;**
- **→ health insurance ID number/medical ID number;**
- **→ mother's maiden name;**
- **→ bank/other financial institution account number;**
- **→ date of birth;**
- **→ personal identification number;**
- **→ unique biometric data including fingerprint, voice print, retina or iris image or other unique physical representation;**
- **→ credit card number; or**
- **→ other payment device number.**

Instructor Notes:

The text of CR § 8-301 has been formatted with emphasis added for instructional purposes.

(PPT SLIDES # 86-108)

TRAINING OBJECTIVE:

Define the term IDENTITY THEFT.

DEFINITIONS

PAYMENT DEVICE NUMBER

(PPT SLIDE # 9)

PERSONAL IDENTIFYING INFORMATION

Instructor Note:

Health insurance ID number and medical ID number and "unique biometric data…added to law effective October 1, 2013.

(6) "RE-ENCODER" means an:
→ ELECTRONIC device that places ENCODED PERSONAL IDENTIFYING INFORMATION OR A PAYMENT DEVICE NUMBER:
- FROM THE MAGNETIC STRIP/STRIPE OF A CREDIT CARD:
  - ► ONTO THE MAGNETIC STRIP/STRIPE OF A DIFFERENTCREDIT CARD OR ANY ELECTRONIC MEDIUM or allows such a transaction to occur.

(PPT SLIDE # 90)

RE-ENCODER

(7) "SKIMMING DEVICE" means a:
→ SCANNER, SKIMMER, READER, OR ANY OTHER ELECTRONIC DEVICE that is used to:
- ■ ACCESS, READ, SCAN, OBTAIN, MEMORIZE, OR STORE:
  - ● TEMPORARILY OR PERMANENTLY
    - ★ PERSONAL IDENTIFYING INFORMATION OR A PAYMENT DEVICE NUMBER ENCODED ON THE MAGNETIC STRIP/STRIPE OF A CREDIT CARD.

SKIMMING DEVICE

(PPT SLIDE # 90)

CR § 8-201 Definitions.

(c) *Credit Card.*

(1) Credit card means an:
→ instrument or device issued by an issuer for the use of a cardholder in obtaining money, goods, services, or anything of value on credit.

(2) "Credit card" includes:
(i) a debit card, access card or other device for use by a cardholder to effect a transfer of funds through an electronic terminal, telephone or computer;
(ii) a magnetic tape that orders or authorizes a financial institution to debit or credit an account; and
(iii) a code, account number, or other means of account access that is not encoded or truncated and can be used to:
1. obtain money, goods, services or anything of value; or
2. initiate a transfer of funds.

(3) "Credit card does NOT include a check, draft, or similar paper instrument.

Instructor Note:

In as much as the term "Credit Card" is used in Subtitle 3 – Identity Fraud, its definition as presented in CR § 8-201 (c) is included in this section of the lesson plan.

CR § 8-301

(b) ***PROHIBITED*** – ***OBTAINING PERSONAL IDENTIFYING INFORMATION WITHOUT CONSENT.***

A person may ***NOT*** KNOWINGLY, WILLFULLY, AND WITH FRAUDLENT INTENT:

- → POSSESS
- → OBTAIN, or
- → HELP ANOTHER PERSON TO POSSESS OR OBTAIN:
  - ► ANY PERSONAL IDENTIFYING INFORMATION OF AN INDIVIDUAL:
    - • ***WITHOUT*** THE CONSENT OF THE INDIVIDUAL IN ORDER TO:
      - ■ USE
      - ■ SELL, or
      - ■ TRANSFER:
        - ▪ THE INFORMATION TO GET A:
          - ✶ BENEFIT
          - ✶ CREDIT
          - ✶ GOOD
          - ✶ SERVICE, or
          - ✶ OTHER THING OF VALUE
            - ◆ IN THE NAME OF THE INDIVIDUAL: or
      - ■ ACCESS HEALTH INFORMATION OR HEALTH CARE IN THE NAME OF THE INDIVIDUAL.

(c) ***PROHIBITED*** – ***ASSUMING IDENTITY OF ANOTHER.***

A person may ***NOT*** KNOWINGLY AND WILLFULLY ASSUME THE IDENTITY OF ANOTHER, INCLUDING A FICTITIOUS PERSON:

(1) TO AVOID IDENTIFICATION, APPREHENSION, OR PROSECUTION FOR A CRIME; or

(2) WITH FRAUDULENT INTENT TO:

(i) GET A BENEFIT, CREDIT, GOOD, SERVICE, OR OTHER THING OF VALUE;

(ii) ACCES TO HEALTH INFORMATION AND HEALTH CARE; or

(iii) AVOID THE PAYMENT OF DEBT OR OTHER LEGAL OBLIGATION.

(PPT SLIDE # 87)

PROHIBITED ACTS

OBTAINING PERSONAL INDENTIFYING INFORMATION

TRAINING OBJECTIVE:

Given various criminal situations demonstrate ability to identify elements of a given crime, utilizing the Annotated Code of Maryland and/or the Digest of Criminal Laws, that enable an officer to make a warrantless arrest.

Identify the basic elements of the crime of identity theft/fraud as contained in the Annotated Code of Maryland.

(PPT SLIDE # 88)

ASSUMING THE IDENTITY OF ANOTHER

Instructor Note:

The words "including a fictitious person" were added to CR § 8-301 (c) during the 2011 session of the Maryland General Assembly. This change became effective October 1, 2011. "Access to health information and health care" added to the law effective October 1, 2013.

(d) ***USE of re-encoder or skimming device.***

A person may NOT knowingly, willfully, and with fraudulent intent to obtain a benefit, credit, good, service or other thing of value or to access health information or care use:

(1) a ***RE-ENCODER*** to place information encoded on the magnetic strip or stripe of a credit card onto the magnetic strip or stripe of a different credit card, or use any OTHER ELECTRONIC MEDIUM that allows such a transaction to occur:

→ ***WITHOUT*** THE CONSENT OF THE INDIVIDUAL AUTHORIZED TO USE THE CREDIT CARD from which the personal identifying information or payment device is being re-encoded; or

(2) a ***SKIMMING DEVICE*** to ACCESS, READ, SCAN, OBTAIN, MEMORIZE, OR STORE personal information or a payment device number on the magnetic strip or stripe of a credit card:

→ ***WITHOUT*** THE CONSENT OF THE INDIVIDUAL AUTHORIZED TO USE THE CREDIT CARD.

(e) ***POSSESSION of re-encoder or skimming device.***

A persons may ***NOT*** knowingly, willfully and with fraudulent intent POSSESS, OBTAIN, OR HELP ANOTHER POSSESS OR OBTAIN A RE-ENCODER DEVICE or a SKIMMING DEVICE for the unauthorized use, sale, or transfer of personal identifying information or a payment device number.

(f) ***Representation without authorization prohibited.***

A person may NOT knowingly and willfully claim to represent another person:

→ ***WITHOUT*** THE KNOWLEDGE AND CONSENT OF THAT PERSON:

- WITH THE INTENT TO SOLICIT, REQUEST, OR TAKE ANY OTHER ACTION TO OTHERWISE INDUCE ANOTHER PERSON TO PROVIDE PERSONAL IDENTIFYING INFORMATION OR A PAYMENT DEVICE NUMBER.

(PPT SLIDES # 92-93)

USING/POSSESSING DEVICES TO FRAUDLENTLY OBTAIN PERSONAL IDENTIFYING INFORMATION

(PPT SLIDE # 88)

CR § 8-301 (g) ***Penalty.***

(1) (i) A person who violates this section where the benefit, credit, good, service, health information or care or other thing of value that is subject of subsection (b), (c), or (d) that has a value of:

- → at least $1,000 but less than $10,000 is guilty of a ***FELONY;***
- → at least $10,000 but less than $100,000 is guilty of a ***FELONY;***
- → $100,000 or more is guilty of a ***FELONY;***

(2) → has a value of less than $1,000 is guilty of a ***MISDEMEANOR;***

(3) A person who violates this section under circumstances that reasonably indicate that the person's intent was to:

- → MANUFACTURE
- → DISTRIBUTE, or
- → DISPENSE ANOTHER INDIVIDUAL'S PERSONAL IDENTIFYING INFORMATION:
  - ■ WITHOUT THAT INDIVIDUAL'S CONSENT

is guilty of a ***FELONY;***

(4) A person who violates subsection (c) (1), (e), or (f) of this section is guilty of a ***MISDEMEANOR;***

(5) When the violation of this section is pursuant to one scheme or continuing course of conduct, whether from the same or several sources, the conduct may be considered one violation and the value of the benefit, credit, good, service or other thing of value may be aggregated in determining whether the violation is a felony or misdemeanor.

RELATED OFFENSES:

CREDIT CARD CRIMES
MARYLAND ANNOTATED CODE
CRIMINAL LAW ARTICLE
TITLE 8 – FRAUD AND RELATED CRIMES
SUBTITLE 2 – CREDIT CARD CRIMES

✓ Maryland law [CR § 8-201 et al.] makes it a criminal offense to:

→ make a false statement in writing about identity of person or of another to procure issuance of credit card; [CR § 8-203 - MISDEMEANOR]

PENALTIES

(PPT SLIDE # 94)

INSTRUCTOR NOTE:

Reference to the different monetary values reflects the different sentences that can be imposed upon conviction for that particular theft.
The cited monetary values are effective October 1, 2013.

(PPT SLIDES # 98-102)

→ take credit card without consent of cardholder; **[CR § 8-204 (a) (1) (i) - MISDEMEANOR]** **→ receive credit card with intent to use/sell/transfer it to another who is not issuer or cardholder;** **[CR § 8-204 (a) (1) (ii) - MISDEMEANOR]** **→ receive credit card that person knows was lost/mislaid/delivered under mistake as the identity or address of cardholder and retain possession of credit card with intent to use/sell/transfer it to another who is not issuer of card;** **[CR § 8-204 (b) (1) - MISDEMEANOR]** **→ sell credit card unless person is issuer;** **[CR § 8-204 (c) (1) - MISDEMEANOR]** **→ buy credit card from person other than issuer;** **[CR § 8-204 (c) (2) - MISDEMEANOR]** **→ receive credit card person knows was taken/retained under circumstances that constitute:** **(1) credit card theft;** **(2) violation of CR § 8-203;** **[CR § 8-204 (d) (1) – MISDEMEANOR]** **(3) violation of CR § 8-204 (c);** **[CR § 8-204 (d) (2) – MISDEMEANOR]** **→ with intent to defraud another:** **(1) falsely make a purported credit card;** **[CR § 8-205 (b) (1) – FELONY]** **(2) falsely emboss a credit card;** **[CR § 8-205 (b) (2) – FELONY]** **(3) transfer or possess:** **(i) falsely made instrument/device that purports to be credit card with knowledge that the instrument/device was falsely made;** **[CR § 8-205 (b) (3) (i) – FELONY]** **(ii) falsely embossed credit card with knowledge that credit card was falsely made or falsely embossed;** **[CR § 8-205 (b) (3) (ii) - FELONY]** **→ sign credit card with intent to defraud another if not cardholder/anyone authorized by cardholder;** **[CR § 8-205 (c) - FELONY]**	

→ for purpose of obtaining money/goods/services/anything of value with intent to defraud another use: **(1) credit card obtained/retained in violation of § 8-204 or § 8-205 of this subtitle; or** **(2) credit card person knows is counterfeit;** **[CR § 8-206 (a) (1) and (2) – FELONY/MISDEMEANOR depending on value]** **→ with intent to defraud another/obtain money/goods/services/anything of value by representing:** **(1) without consent of cardholder that the person is the holder of a specified credit card; or** **(2) the person is holder of a credit card when the credit card had not been issued;** **[CR § 8-206 (b) (1) and (2) – FELONY/MISDEMEANOR depending on value]** **→ person/agent/employee of person authorized by issuer to furnish money/goods/services/anything of value on presentation of credit card by cardholder with intent to defraud the issuer or cardholder:** **(1) furnish money/goods/services/anything of value on presentation of:** **(i) credit card obtained/retained in violation of § 8-204 or § 8-205 of this subtitle; or** **(ii) credit card the person knows is counterfeit;** **[CR § 8-207 (a) (i) and (ii) – FELONY/MISDEMEANOR depending on value]** **(2) fail to furnish money/goods/services/anything of value that the person represents in writing to the issuer that the person has furnished;** **[CR § 8-207 (2) – FELONY/MISDEMEANOR depending on value]** **→ person other than cardholder without consent of issuer possess incomplete credit card with intent to complete it; [CR § 8-208 (b) (1) – FELONY]** **→ possess with knowledge of its character machinery/plates/any other contrivance designed to reproduce instrument purporting to be a credit card or issuer that not consented to preparation of the credit card; [CR § 8-208 (b) (2) – FELONY]**	

→ receive money/goods/services/anything of value if person knows/believes money/goods/services/anything of value was obtained in violation of § 8-206 of this subtitle; [CR § 8-209 (a) – FELONY/MISDEMEANOR depending on value] **→ publish or cause to be published [communicate information to one or more persons either orally in person/by telephone/radio/television or in writing of any kind]:** **► number/code of existing/canceled/revoked/expired/nonexistent telephone credit card; or** **► numbering/coding system that is used in issuing telephone credit cards:** **✶ with intent that the number/code/system be used with knowledge that it may be used fraudulently to avoid paying lawful toll charge;** **[CR § 8-210 (b) – MISDEMEANOR]** **→ use/disclose any credit card number/other payment device number/holder's signature <u>unless</u>:** **(1) person is holder of credit card number/payment device number;** **(2) disclosure is made to holder/issuer of credit card number/payment device number;** **(3) use/disclosure is:** **(i) required under federal or State law;** **(ii) at direction of a governmental unit in accordance with law; or** **(iii) in response to the order of the court having jurisdiction to issue the order;** **(4) disclosure is in connection with:** **► authorization, processing, billing, collection, chargeback, insurance collection, fraud prevention, or credit card/payment device recovery that relates to credit card number or payment device number;** **► account accessed by credit card number/payment account number** **► debt for which the holder or person authorized by holder gave credit card number/payment device number for purposes of identification; or** **► debt/obligation arising alone/in conjunction with another means of payment from use of credit card number/payment device number;** **[CR § 8-214 (a) (1) (2) (3) (4)]**	**[SEE COMPLETE TEXT OF CR § 8-214 FOR OTHER PROHIBITED DISCLOSURES]**

BLANK IDENTIFICATION CARDS **CR § 8-302** **GOVERNMENT IDENTIFICATION DOCUMENTS** **CR § 8-303** ✓ **CR § 8-302. Blank or incorrect identification card.** **(b) ...a person may not:** **(1) sell/issue/offer for sale/offer to issue identification card/document that contains:** **(i) blank space for person's age/date of birth; or** **(ii) person's incorrect age/date of birth; or** **(2) knowingly sell/issue/offer for sale/offer to issue identification card/document that contains:** **(i) incorrect name instead of person's true name; or** **(ii) incorrect address for person; [MISDEMEANOR]** **Exception:** **This section does not prohibit a manufacturer of identification cards/documents from selling/issuing identification cards/documents that contain a blank space for a person's age/date of birth to:** **(1) employers for use as employee identification cards/documents;** **(2) hospitals for use as patient identification cards;** **(3) governmental units.** **(d) EACH IDENTIFICATION CARD/DOCUMENT SOLD OR ISSUED AND EACH OFFER IN VIOLATION OF THIS SECTION IS A CRIME THAT MAY BE *SEPARATELY* PROSECUTED.**	**(PPT SLIDES # 95 - 97)** **(PPT SLIDE # 96)**

✓ **§ 8-303. Government identification document.** **(a) Government identification document means one of the following documents issued by the United States government or any state/local government:** **(1) passport;** **(2) immigration visa;** **(3) alien registration card;** **(4) employment authorization card;** **(5) birth certificate;** **(6) Social Security card;** **(7) military identification;** **(8) adoption decree;** **(9) marriage license;** **(10) driver's license;** **(11) photo identification card;** **(b) a person may NOT with fraudulent intent:** **(1) POSSESS a fictitious or fraudulently altered government identification document;** **(2) DISPLAY/cause/allow to be displayed a fictitious or fraudulently altered government identification document;** **(3) LEND a government identification document to another or knowingly allow the use of the person's government identification document by another; or** **(4) DISPLAY or REPRESENT as the person's own a government identification document not issued to the person. [MISDEMEANOR]**	**(PPT SLIDE # 97)**

AUTHORITY TO INVESTIGATE:

(PPT SLIDES # 103-106)

AUTHORITY TO INVESTIGATE

(PPT SLIDE # 104)

✓ **CR § 8-301:**

(k) ***Statewide jurisdiction for officers – STATE POLICE.***

Notwithstanding any other law, the Department of State Police may initiate investigations and enforce this section throughout the state:

- → ***WITHOUT*** **REGARD TO ANY LIMITATION OTHERWISE APPLICABLE TO THE DEPARTMENT'S ACTIVITIES IN A MUNICIPAL CORPORATION OR OTHER POLICTICAL SUBDIVISION.**

(l) ***Statewide jurisdiction for officers – OTHER OFFICERS.***

(1) Notwithstanding other law, a LAW ENFORCEMENT OFFICER OF:

- → **the Maryland Transportation Authority Police;**
- → **the Maryland Port Administration Police;**
- → **the Park Police of the Maryland –National Capital Park and Planning Commission; or**
- → **a MUNICIPAL CORPORATION; or**
- → **COUNTY;**

MAY INVESTIGATE VIOLATIONS OF THIS SECTION:

- → ***THROUGHOUT THE STATE:***
  - ✶ **WITHOUT ANY LIMITATION AS TO JURISDICTION, and**
  - ✶ **TO THE SAME EXTENT AS A LAW ENFORCEMENT OFFICER OF THE DEPARTMENT OF STATE POLICE.**

TERMINAL OBJECTIVE:

Identify the basic responsibility of the officer when Investigating the crime of identity theft.

(2) The authority granted in paragraph (1) of this subsection may be exercised only in accordance with regulations that the Department of State Police adopts.

(PPT SLIDE # 105)

NOTIFICATION OF INVESTIGATION

(3) The regulations are *not* subject to Title 10, Subtitle 1 of the State Government Article.

(4) The AUTHORITY GRANTED in paragraph (1) of this subsection MAY BE EXERCISED ONLY IF:

- → **AN ACT RELATED TO THE CRIME WAS COMMITTED IN THE INVESTIGATING LAW ENFORCEMENT AGENCY'S JURISDICTION; or**
- → **the COMPLAINING WITNESS RESIDES IN THE INVESTIGATING LAW ENFORCEMENT AGENCY'S JURISDICTION.**

(5) during investigation, officer remains an employee of officer's employing agency;

(m) ***Required notifications.*** If action is taken under the authority granted in subsection (l) of this section, notification of an investigation: (1) IN A MUNICIPAL CORPORATION, shall be made to the chief of police/designee of the chief of police; (2) IN A COUNTY THAT HAS A COUNTY POLICE DEPARTMENT, shall be made to the chief of police or designee of the chief of police; (3) IN A COUNTY ***WITHOUT*** A POLICE DEPARTMENT shall be made to the sheriff/designee of the sheriff; (4) IN BALTIMORE CITY, shall be made to the Police Commissioner/the Police Commissioner's designee; (5) ON PROPERTY OWNED, LEASED OR OPERATED BY OR UNDER THE CONTROL OF THE MARYLAND TRANSPORTATION AUTHORITY, THE MARYLAND AVIATION ADMINISTRATION OR THE MARYLAND PORT ADMINISTRATION, shall be made to the respective chief of police/the chief's designee; and (6) ON PROPERTY OWNED, LEASED OR OPERATED BY OR UNDER THE CONTROL OF THE MARYLAND-NATIONAL CAPITAL PARK AND PLANNING COMMISSION to the chief of police of the Maryland-National Capital Park and Planning Commission for the county in which the property is located.	(PPT SLIDE # 106)
(o) *Investigation and prosecution.* (1) A STATE'S ATTORNEY or the ATTORNEY GENERAL may ***investigate*** and ***prosecute*** a violation of this section or a violation of any crime based on the act establishing a violation of this section. (2) If the Attorney General exercises authority under paragraph (1) of this subsection, the Attorney General has all the powers and duties of a State's Attorney, including the use of a grand jury in any county or Baltimore City, to investigate and prosecute the violation.	(PPT SLIDES # 107-108) ***INVESTIGATION AND PROSECUTION***
(p) *Venue.* Notwithstanding any other provision of law, the prosecution of a violation of any crime based on the act establishing a violation of this section may be commenced in any county in which: (1) an element of the crime occurred; (2) the victim resides.	

IDENTITY THEFT/FRAUD – REPORTING:

OVERVIEW:

(PPT SLIDES # 109-110)

✓ identity theft/fraud is a NON-TRADITIONAL CRIME:
- → NOT specifically recorded as an offense category in the FBI's Uniform Crime Reporting (UCR) program;
- → many states continue to lack comprehensive data on the numbers of identity theft crimes that have occurred: and the number of arrests/convictions that have resulted from investigations into these crimes;

✓ local police have the first official contact with the victim of identity theft and their preliminary investigation as reflected in their incident/offense report can be an important investigative resource;

(PPT SLIDES # 111 -113)

✓ police reports of identity theft serve two important purposes:
- → important first step in the investigation of the crime;
- → serve the victim as documentation to his/her creditor and/or debt collectors that the crime has been reported;

MARYLAND LAW:

✓ the State of Maryland has attempted to address both the need for official documentation of the crime of identity theft by the victim and the need to develop meaningful statistical data regarding the occurrence of the various forms of identity theft throughout the State through various legislation:

→ in 2005, the Maryland Legislature enacted and the Governor signed into law CR § - 8 – 304. Report which requires law enforcement officers to complete a report of *any* incident of IDENTITY THEFT/FRAUD regardless of whether the offense occurred/did not occur in the jurisdiction of the officer taking the report:

CR § 8-304. Report.

(a) *Contact local law enforcement agency.*
A person who knows or reasonably suspects that the person is a victim of identity fraud, as prohibited under this subtitle, may contact a LOCAL LAW ENFORCEMENT AGENCY THAT HAS JURISDICTION OVER:
(1) ANY PART OF THE COUNTY IN WHICH THE *PERSON LIVES*; OR
(2) ANY PART OF THE COUNTY IN WHICH THE *CRIME OCCURRED*.

TERMINAL OBJECTIVE:

Identify the basic responsibility of the officer when investigating the crime of identity theft.

Instructor Note:

The requirement established by CR § 8-304 that law enforcement officers complete a report of an incident involving identity theft regardless of where the offense occurred may conflict with an agency's standard operating procedure regarding the reporting of out-of-jurisdiction offenses/incidents.

This exception to an agency's reporting policy/procedures should be pointed out/explained to recruits.

(b) *Preparation of report.*
After being contacted by a person in accordance with subsection (a) of this section, A LOCAL LAW ENFORCEMENT AGENCY SHALL PROMPLTY:
(1) PREPARE AND FILE A REPORT OF THE ALLEGED IDENTITY FRAUD; and
(2) ***PROVIDE*** A COPY OF THE REPORT TO THE VICTIM.

(c) *Refer matter to another law enforcement agency.*
The local law enforcement agency contacted by the victim ***may*** subsequently refer the matter to a law enforcement agency with proper jurisdiction.

(d) *Not included as open case.*
A report filed under this section is not required to be counted as an open case for purposes including compiling open case statistics.

✓ in addition to the reporting requirements imposed by CR § 8-304 the State of Maryland has developed a uniform reporting form for offenses involving identity theft:

Public Safety Article
Title 3
Subtitle 2
Police Training Commission

PS § 3 – 207. General Powers and Duties of Commission.

Subject to the authority of the Secretary, the Commission has the following powers and duties:

(16) to develop, with the cooperation of the Office of the Attorney General, the Governor's Office of Crime Control and Prevention and the Federal Trade Commission, a UNIFORM IDENTITY FRAUD REPORTING FORM that:
(I) makes transmitted data available on or before October 1, 2011 for use by each law enforcement agency of State and local government; and
(II) may authorize the data to be transmitted to the Consumer Sentinel Program in the Federal Trade Commission.

Demonstrate completion of acceptable police reports for various offenses, incidents, or situations.

Apply the law as contained in the Annotated Code of Maryland that requires a law enforcement officer to prepare and file a report from the victim of identity/theft/fraud.

Given a scenario involving identity theft/fraud, compose a complete *initial* identity theft/fraud offense report that includes, at a minimum, the following elements:
- complete victim information at the time of the identity theft/fraud;
- complete description of the type of item/identity document stolen/compromised;
- specific information about how the stolen/compromised identity item/document was discovered by the victim and how the identity item/document was used;
- potential suspect information;
- action victim has taken to mitigate the identity loss/compromise; and
- description of recommended follow-up action given to the victim.

UNIFORM REPORT – IDENTITY FRAUD/THEFT

ANNOTATED CODE OF MARYLAND

Article – PUBLIC SAFETY

Background:

During the 2010 legislative session the Maryland Legislature repealed and reenacted, with amendments:

Public Safety Article
Title 3 – Law Enforcement
Subtitle 2 – Police Training Commission
§ 3 – 207 General Power and Duties of Commission
Annotated Code of Maryland
(2003 Volume and 2009 Supplement)

Among other changes, § 3-207 - "General powers and duties of Commission" contains the following provision regarding the development and distribution of a *uniform* Identity Fraud Reporting form:

> **Subject to the authority of the Secretary, the Commission has the following powers and duties:**
>
> **(16) to develop, with the cooperation of the Office of the Attorney General, the Governor's Office of Crime Control and Prevention and the Federal Trade Commission, a uniform identity fraud reporting form that:**
> **(i) makes transmitted data available on or before October 1, 2011, for use by each law enforcement agency of State and local government; and**
> **(ii) may authorize the data to be transmitted to the Consumer Sentinel Program in the Federal Trade Commission;**

Action Taken:

As required by law, the Maryland Police and Correctional Training Commission, in consultation with the Office of the Attorney General, Consumer Protection Division, and the Governor's Office of Crime Control Prevention, Maryland Statistical Analysis Center, and the Federal Trade Commission has developed the captioned uniform IDENTITY FRAUD/THEFT reporting form.

The uniform IDENTITY FRAUD/THEFT reporting form has been developed using a variety of sources including the following:

> **Identity Theft Victims' Universal Complaint Form**
> **(Federal Trade Commission)**
> **Identity Crime Incident Detail Form**
> **(U.S. Secret Service)**
> **Model Policy – Identity Crime**
> **(International Association of Chiefs of Police)**
> **Application for Maryland Identity Theft Passport**
> **(Office of Maryland Attorney General)**

INSTRUCTIONS FOR COMPLETING FORM

PAGE 1 - LINES # 1-2: *Reporting* Agency Identifiers.

PAGE 1 - LINE # 3: Agency Complaint/Case Number.

PAGE 1 - LINE # 4: Date report taken.

PAGE 1 - LINES # 5-11: Victim Identification – to be completed as indicated on form.

PAGE 2 - BLOCK # 12: Determine if document/information was stolen or lost.

PAGE 2 - BLOCKS # 13-14: To be completed as indicated on form.

PAGE 2 - BLOCK # 15: Determine HOW victim discovered theft/compromise occurred – check all that apply.

PAGE 2 - BLOCK # 16: Determine identity information/item compromised – check all that apply.

PAGE 3 - BLOCK # 17: Determine from victim if information/identity was used to:

- **establish *NEW* account;**
- **use an *EXISTING* account;**

✶ Note: Use separate pages if multiple/additional accounts are involved.

PAGE 4 - BLOCK # 18: Obtain a *detailed* narrative from victim to include as much of the information contained in BLOCK # 18 as possible. Use additional page(s) if necessary.

PAGE 5 - BLOCK # 19: Determine from victim the names/identities of any "potential suspect(s).

PAGE 5 - LINE # 20: To be completed as indicated on form.

PAGE 5 - LINE # 21: To be completed as indicated on form if known.

PAGE 6 - BLOCK # 22: Page to be given to victim as reference/resource:

✶ Note: Reporting officer should explain options/recommended actions to the victim if necessary.

ANNOTATED CODE OF MARYLAND

CR § 8-304. REPORT.

(a) Contact local law enforcement agency. – A person who knows or reasonably suspects that the person is a victim of identity fraud, as prohibited under this subtitle, may contact a local law enforcement agency that has jurisdiction over:

(1) any part of the county in which the person lives; or,

(2) any part of the county in which the crime occurred.

(b) Preparation of report. – After being contacted by a person in accordance with subsection(a) of this section, a local law enforcement agency shall promptly:

(1) prepare and file a report of the alleged identity fraud; and,

(2) PROVIDE A COPY OF THE REPORT TO THE VICTIM.

3/31/11

UNIFORM IDENTITY FRAUD/THEFT REPORTING FORM

LAW ENFORCEMENT AGENCY IDENTIFIERS/ADMINISTRATIVE INFORMATION

1. AGENCY NAME:	**2. REPORTING AGENCY ORI #:**
3. COMPLAINT/INCIDENT/REPORT #:	**4. DATE REPORT TAKEN:**

VICTIM INFORMATION

5. LEGAL NAME OF VICTIM AT TIME OF REPORT:

_____ _____ _____
(last) **(first)** **(middle)**

6. DATE OF BIRTH: _____

7. VICTIM CURRENT ADDRESS:

_____
(STREET NAME/APARTMENT #)

_____
(CITY) **(STATE)** **(ZIP CODE)**

8. TELPHONE #:

_____ _____ _____
(home) **(work)** **(cell – optional)**

9. "E" MAIL ADDRESS (recommended/not required)

10. DRIVER LICENSE INFORMATION:

_____ _____
(number) **(state of issuance)**

11. VICTIM FULL LEGAL NAME AT TIME OF THEFT/DISCOVERY OF THEFT *IF DIFFERENT FROM ABOVE:*

_____ _____ _____
(last) **(first)** **(middle)**

PERSONAL INFORMATION - IDENTITY THEFT/COMPROMISE SUMMARY

12. DOCUMENT/INSTRUMENT/INFORMATION:

____ LOST ____ STOLEN

___ UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION FROM OTHER RECORDS:

TYPE OF RECORD: _____

13. DATE IDENTITY THEFT FIRST *NOTICED/DISCOVERED:*

AMOUNT OF MONEY SPENT TO DATE TO RESOLVE THEFT (ESTIMATE IF NOT SURE): $_____

AMOUNT OF TIME SPENT TO DATE TO RESOLVE THEFT (ESTIMATE IF NOT SURE): _____
(HOURS)

14. LOCATION/ADDRESS IDENTITY THEFT/LOSS BELIEVED TO HAVE OCCURRED:

_____
(STREET)

_____
(CITY) (COUNTY) (STATE) (ZIPCODE)

IF COMMERCIAL ESTABLISHMENT – NAME:_____

15. IDENTITY THEFT/COMPROMISE DISCOVERED HOW (CHECK APPLICABLE):

____ SELF-INITIATED CREDIT REPORT CHECK
____ FRAUDULENT/UNAUTHORIZED ACCOUNT:
___ OPENED ___ USED
____ OVERDRAWN ACCOUNT
____ CREDIT REPORT FINDING BY FINANCIAL/OTHER INSTITUTION
____ NOTIFIED BY:
_____ BANK/CREDIT UNION/OTHER TYPE OF FINANCIAL INSTITUTION
_____ CREDIT CARD COMPANY/OTHER CREDITOR
_____ BILL COLLECTION AGENCY/REPRESENTATIVE
_____ INSURANCE COMPANY
_____ UTILITY/TELEPHONE COMPANY
____ DENIED LOAN/CREDIT
____ ARRESTED/HAD WARRANT ISSUED/COMPLAINT FILED FOR CRIME DID *NOT* COMMIT
____ DRIVER'S LICENSE SUSPENDED FOR ACTS *NOT* COMMITTED
____ SUED FOR DEBT *NOT* INCURRED
____ DENIED EMPLOYMENT FOR FINANCIAL REASONS
____ THEFT OF MAIL/DIVERSION OF MAIL FROM ADDRESS
____ GARBAGE/RECYCLABLES GONE THROUGH
____ OTHER (DESCRIBE): _____

16. TYPE OF IDENTITY INFORMATION/ITEM COMPROMISED (CHECK APPLICABLE TYPES):

____ SOCIAL SECURITY NUMBER
____ DRIVER'S LICENSE
____ BIRTH CERTIFICATE/OTHER
____ RESIDENT ALIEN CARD
____ PASSPORT
____ EDUCATIONAL RECORDS
____ MEDICAL RECORDS
____ PROFESSIONAL RECORDS/LICENSE
____ INSURANCE RECORDS:
____ MEDICAL
____ OTHER (IDENTIFY TYPE):
_____

____ UTILITIES/TELEPHONE RECORDS
____ ATM/BANK CARD
____ SAVINGS ACCOUNT
____ CREDIT CARD
____ CHECKING ACCOUNT
____ BROKERAGE/STOCK ACCOUNT
____ PERSONAL COMPUTER:
____ INTERNET PURCHASE
____ FILES HACKED
____ OTHER (PROVIDE INFORMATION):
_____

17. HOW INFORMATION/IDENTITY WAS USED (CHECK APPLICABLE):

____ *NEW* ACCOUNT:

____ FRAUDULENTLY ATTEMPTED TO OPEN *NEW* ACCOUNT (fill in applicable information)

____ FRAUDULENTLY OPENED *NEW* ACCOUNT (fill in applicable information)

- **DATE OPENED: _____**
- **TYPE OF ACCOUNT: _____**

- **COMPANY NAME: _____**
  - **ACCOUNT #: _____**
  - **AMOUNT OBTAINED/CREDIT LIMIT: $_____**
- **COMPANY ADRESS: _____**
- **COMPANY PHONE #: _____**
- **COMPANY "E" MAIL ADDRESS:_____**

- **TYPE OF FRAUD/THEFT:**
  - **____ CASH OBTAINED: $_____**
  - **____ MERCHANDISE OBTAINED: $_____**
  - **____ SERVICES OBTAINED:**
    - **____ GOVERNMENT BENEFITS;**
    - **____ MEDICAL SERVICES;**
    - **____ OTHER: _____**

____ *EXISTING* ACCOUNT:

____ FRAUDULENTLY ATTEMPTED TO USE *EXISITING* ACCOUNT (fill in applicable information)

____ FRAUDULENTLY USED *EXISTING* ACCOUNT (fill in applicable information)

- **TYPE OF ACCOUNT: _____**

- **COMPANY NAME: _____**
  - **ACCOUNT #: _____**
  - **AMOUNT OBTAINED/CREDIT LIMIT: $_____**
- **COMPANY ADRESS: _____**
- **COMPANY PHONE #: _____**
- **COMPANY "E" MAIL ADDRESS:_____**
- **ACCOUNT #: _____**

- **DATE(S) ACCOUNT WAS USED: _____**

TYPE OF FRAUD/THEFT:

- **____ CASH OBTAINED: $_____**
- **____ MERCANDISE OBTAINED: $_____**
- **____ SERVICES OBTAINED:**
  - **____ GOVERNMENT BENEFITS**
  - **____ MEDICAL SERVICES**
  - **____ OTHER: _____**

[LIST ADDITIONAL/MULTIPLE STOLEN/COMPROMISED ACCOUNTS ON SEPARATE PAGES]

VICTIM ACCOUNT/NARRATIVE OF HOW THEFT OCCURRED OR DISCOVERED & ACTION TAKEN

18. DETAILED NARRATIVE FROM VICTIM – INCLUDE THE FOLLOWING INFORMATION IF APPLICABLE:

- **LOCATION IDENTITY THEFT/LOSS BELIEVED TO HAVE OCCURRED**
- **DESCRIPTION OF PERSONAL INFORMATION LOST/STOLEN/COMPROMISED:**
  - **OTHER/ADDITIONAL IDENTITY INFORMATION LOST/STOLEN COMPROMISED**
- **DETERMINE IF VICTIM AUTHORIZED ANYONE TO USE NAME/PERSONAL INFORMATION:**
  - **IDENTIFY AUTHORIZED USER**
- **DATE THEFT/COMPROMISE OCCURRED/DISCOVERED**
- **EXPLANATION OF HOW THEFT/LOSS/COMPROMISE WAS *DISCOVERED***
- **EXPLANATION OF HOW ACCESS WAS GAINED TO IDENTITY INFORMATION (if known)**
- **WAS IDENTITY THEFT RESULT OF ANOTHER CRIME:**
  ___ BURGLARY ___ STOLEN AUTO ___ ROBBERY ___ OTHER TYPE THEFT
- **DATE/TIME *OTHER* CRIME OCCURRED:**
  - **INCIDENT # (if known)**
- **DESCRIPTION OF HOW PERSONAL INFORMATION WAS USED/FOR WHAT PURPOSE**
- **AMOUNT OF FINANCIAL LOSS (known at time of this report)**
- **IF INTERNET PURCHASE - WEBSITE ADDRESS/COMPANY**
- **NAME/TELEPHONE # OF COMPANY REPRESENTATIVE/INVESTIGATOR MAKING CONTACT**
- **DATE THEFT/LOSS REPORTED TO COMPANY/INSTITUTION**
- **VICTIM IDENTITY VERIFIED BY REPORTING OFFICER AT TIME OF REPORT:**
  - **METHOD USED: _____**
- **DETERMINE IF VICTIM IS WILLING TO ASSIST IN THE INVESTIGATION/PROSECUTION IF SUSPECT IS IDENTIFIED/ARRESTED/CHARGED:**
  ____YES ____ NO ____NOT SURE AT THIS TIME
- **DETERMINE IF VICTIM HAS FILED A REPORT WITH ANY OTHER LAW ENFORCEMENT AGENCY:**
  - **IF YES, NAME OF AGENCY/REPORT #: _____**
- **DETERMINE IF VICTIM HAS ADDITIONAL DOCUMENTATION TO SUPPORT THEFT/FRAUD CLAIM THAT MIGHT ASSIST IN INVESTIGATION**
  - **IF YES, IDENTIFY DOCUMENT: _____**

NARRATIVE:

"POTENTIAL" SUSPECT INFORMATION

19. "POTENTIAL" SUSPECT IDENTIFIERS:

SUSPECT NAME/ALIAS: _____

SUSPECT ADDRESS: _____

SUSPECT TELEPHONE #: _____

SUSPECT RELATIONSHIP TO VICTIM: _____

METHOD USED TO OBTAIN IDENTITY ITEM (if known/suspected):

AUTHORIZATION BY VICTIM TO SUSPECT TO USE PERSONAL IDENTITY INFORMANTION:
___ YES ___ NO

IF YES, TRANSACTIONS/CIRCUMSTANCES AUTHORIZED FOR (EXPLAIN):

OFFICER CONTACT INFORMATION

20. NAME/ASSIGNMENT/TELEPHONE # *REPORTING* OFFICER:

_____
(NAME) (TELEPHONE #) (E MAIL)

21. NAME/ASSIGNMENT/TELEPHONE # OF FOLLOW-UP *INVESTIGATOR* (if known):

_____
(NAME) (TELEPHONE #) (E MAIL)

VICTIM ASSISTANCE INFORMATION/CHECKLIST

An Identity Theft Report entitles an identity crime victim to certain important protections that may help the victim eliminate fraudulent debt and restore their credit to pre-crime status. It is recommended that the victim of the identity theft be provided with the following information after the Identity Crime Report has been completed.

Briefly describe the agency investigative process that occurs after an Identity Theft Report is completed.

22. RECOMMENDED ACTION TO BE TAKEN BY VICTIM (CHECK APPLICABLE):

____ **BEGIN *WRITTEN* LOG OF ACTION TAKEN TO INCLUDE:**
- **DATES/TIMES OF CONTACTS**
- **NAMES/TELEPHONE # OF CONTACTS**
- **SUMMARY OF ACTION NEEDED/TAKEN**
- **RECORD TIME SPENT/EXPENSES INCURRED FOR CONTACT**
- **CONFIRM *IN WRITING* ALL CONVERSATIONS REGARDING THEFT/FRAUD/COMPROMISE**
- **MAINTAIN COPIES OF ALL CORRESPONDENCE/DOCUMENTS REGARDING THEFT**

____ **OBTAIN/REVIEW COPY OF CREDIT REPORT(S):**
- **EQUIFAX (800-685-1111) www.equifax.com**
- **EXPERIAN (888-397-3742) www.experian.com**
- **TRANS UNION (800-680-7289) www.transunion.com**

____ **IDENTIFY ALL OPEN FRAUDULENT ACCOUNTS:**
- **IDENTIFY FRAUDULENT ACCOUNT NUMBERS**
- **IDENTIFY FRAUDULENT ADDRESSES/OTHER INFORMATION**

____ **NOTIFY ALL CREDITORS ABOUT IDENTITY FRAUD COMPLAINT:**
- **AUTHORIZE ACCESS TO FRAUDULENT ACCOUT INFORMATION FOR LAW ENFORCEMENT FRAUD INVESTIGATORS**
- **DISPUTE STOLEN ACCOUNTS WITH CREDITORS**
- **REQUEST CREDIT REPORTING AGENCIES BLOCK FRAUDULENT INFORMATION**

____ **PLACE FRAUD ALERT**

____ **PLACE CREDIT FREEZE**

____ **OBTAIN REPLACEMENT CREDIT ACCOUNTS WITH NEW ACCOUNT # FOR EXISTING COMPROMISED ACCOUNTS**

____ **NOTIFY AFFECTED CREDIT CARD COMPANY/BANK/FINANCIAL INSTITUTION**

____ **FILE COMPLAINT WITH FEDERAL TRADE COMMISSION (FTC):**
- **COMPLETE ID THEFT AFFIDAVIT (1-877-438-4338) www.ftc.gov/idtheft**

____ **OBTAIN IDENTITY THEFT PASSPORT:**
- **OFFICE OF MARYLAND ATTORNEY GENERAL:**
  - **IDENTITY THEFT UNIT (410-576-6491) www.IDTheft@oag.state.md.us**

____ **MONITOR CREDIT CARD BILLS FOR EVIDENCE OF FRAUDULENT ACTIVITY:**
- **REPORT ACTIVITY IMMEDIATELY TO CREDIT GRANTOR**

____ **NOTIFY SOCIAL SECURITY ADMINISTRATION IF SS# HAS BEEN COMPROMISED:**
- **(1-800-269-0271)**

____ **NOTIFY MOTOR VEHICLE ADMINISTRATION IF DRIVER'S LICENSE HAS BEEN LOST/STOLEN/COMPROMISED:**
- **(1-800-950-1682)**
- **APPLY FOR "V" RESTRICTION ON DRIVER'S LICENSE FROM MVA;**

____ **CONTACT LOCAL LAW ENFORCEMENT AGENCY IF IDENTITY HAS BEEN USED TO COMMIT CRIMINAL VIOLATIONS:**
- **FILE APPROPRIATE ADMINISTRATIVE REPORT FOR MISIDENTIFICATION:**
  - **LOCAL STATE'S ATTORNEY'S OFFICE www.mdsaa.org**
- **PRIVACY RIGHTS CLEARINGHOUSE:**
  - **(1-619-298-3396) www.privacyrights.org**

[USE THIS PAGE AS A VICTIM ASSISTANCE CHECKLIST]

Personal Information Protection Act (PIPA)
Maryland Annotated Code
Commercial Law
Title 14 – Miscellaneous Consumer Protection Provisions

✓ **the Personal Information Protection Act (PIPA) CL§ 14-3501 et al. was enacted to ensure:**
- → **consumer's personal identifying information is reasonably protected;**
- → **if compromised, consumers are notified so that they can take steps to protect themselves;**

Components of the Statute:

→ **"personal information" is defined as an individual's first and last name in combination with a:**
- ► **Social Security number;**
- ► **driver's license number;**
- ► **financial account number such as:**
  - ● **credit card/debit card number;**
  - ● **access code/password that would permit access to an individual's financial account;**
- ► **individual taxpayer identification number;**

unless encrypted/redacted/otherwise rendered unusable;

→ **"security breach" is defined as the UNAUTHORIZED acquisition of computerized data that compromises the security confidentiality or integrity of personal information;** **[CL § 14-3504 (a)]**

→ **if a business experiences a "security breach" where personal information that may pose a threat to a consumer if the information is misused the business must:**
- ► **conduct a reasonable and prompt good faith investigation to determine whether the compromised information has been or is likely to be misused;**
- ► **if the information may be misused the business shall NOTIFY any affected consumer residing in Maryland:**
  - ● **as soon as reasonably possible after the business conducts its investigation into how the breach of security occurred:**
    - ★ **UNLESS REQUESTED BY LAW ENFORCEMENT TO DELAY NOTIFICATION BECAUSE NOTIFICATION MAY IMPEDE A PENDING CRIMINAL INVESTIGATION OR JEOPARDIZE HOMELAND SECURITY;**

(PPT SLIDES # 114-116)

Instructor Note:

The Maryland law [CL § 14-3501 et al.] that governs the security of personal information (PIPA) is provided for general informational purposes in as much as recruits and other law enforcement officers are consumers and have a vested interest in knowing their rights regarding personal information.

Instructor Note:

The Office of the Maryland Attorney General maintains a list of companies that have experienced and reported a data breach during the past several years.

That listing can be viewed at:
www.oag.state.md.us

click on:
Consumer Protection
click on:
Identity Theft
click on:
Data Breaches

→ notice to the affected consumer must be given: **► IN WRITING:** **• sent to the most recent address of the individual;** **► BY TELEPHONE:** **• at the most recent telephone number; or** **► BY "E" MAIL:** **• if the individual has already consented to receive electronic notice or the business primarily conducts business via the Internet;** **► substitute notice by e mail, posting on the business website or notice to statewide media outlets if the cost of notice would exceed $100,000 or the number of consumers to be notified exceeds 175,000;** **→ notice must contain:** **► description of information compromised;** **► business contact information;** **► toll-free numbers and addresses of each of the 3 credit reporting agencies:** **• Equifax (1-888-766-0008);** **• Experian (1-888-397-3742);** **• TransUnion (1-800-680-7289);** **► toll-free numbers/addresses/websites for the Federal Trade Commission and the Office of the Attorney General;** **► a statement that the individual can obtain information from these sources about steps to avoid identity theft;** **→ prior to sending the notice the business must contact the Office of the Attorney General with:** **► a brief description of the security breach;** **► the number of Maryland residents being notified;** **► what information was compromised;** **► steps the business has taken to restore the integrity of the system;** **► a sample copy of the notice being sent out;** **→ if a business is required to send notice of a security breach to more than 1,000 individuals it must notify each consumer reporting agency that compiles/maintains files on consumers on a nationwide basis;** **→ businesses must also take reasonable steps to protect against unauthorized access to or use of personal information when they are destroying or discarding records that contain personal information;**	

INVESTIGATORY RESOURCES:

FTC - CONSUMER SENTINEL PROGRAM:

✓ the FTC maintains a COMPREHENSIVE WEB SITE devoted to identity theft: www.ftc.gov/IDTheft and includes:
- → information for victims/business and law enforcement;
- → consumer information on how to AVOID/DETECT identity crime;
- → what steps to take if an individual's identity is stolen;

✓ the FTC's national repository of identity theft complaints;
- → database for complaints relating to identity theft investigations;
- → reports of recent identity crime schemes;
- → information on state identity crime laws;
- → "e" mail notifications when complaints relating to areas of interest are entered into the database from other agencies;

✓ Internet access for all local, state, federal law enforcement officers:
- → web-based law enforcement network that provides law enforcement agencies with secure, password protected access to consumer complaints about:
  - ► telemarketing schemes;
  - ► direct mail schemes;
  - ► Internet fraud;

✓ to access law enforcement agencies must sign up and complete a confidentiality agreement;

✓ enables users to:
- → share information;
- → avoid duplication of efforts;
- → formulate rapid responses to new fraud schemes;

✓ contains the Identity Theft Clearinghouse which offers direct Internet access to consumer complaints about Identity Crime in order to:
- → locate victims and perpetrators of identity crime;
- → link reports of identity crime that might otherwise appear to be isolated incidents;
- → identity other federal/state/local agencies involved in a particular investigation;
- → help identify trends regards identity crime;

✓ available at www.ftc.gov/sentinel

(PPT SLIDES # 117-119)

Identify the resources available to the officer while conducting a criminal investigation.

Identify the resources available to the officer for crimes involving identity theft/fraud.

TERMINAL OBJECTIVE:

Identify the basic responsibility of the officer when Investigating the crime of identity theft.

Instructor Note:

This lesson plan is intended to provide law enforcement officers with a basic understanding of Identity Theft/fraud. It is not intended as training for investigators who are assigned to investigate identity theft rings or schemes.

Information on the FTC's Consumer Sentinel Program is presented as general law enforcement information.

Individual law enforcement agencies have the option of participating in the Consumer Sentinel Program.

Enrollment into the Program can be made at: www.ftc.gov/sentinel

CREDIT CARD COMPANY DATABASES: ✓ credit issuing and reporting companies maintain databases of lost or stolen cards: → access is available working with local banks and businesses with ties to the credit card companies; **MULTI-AGENCY TASK FORCE:** ✓ coordinates response of various local agencies; **LAW ENFORCEMENT TRAINING AND INVESTIGATIVE RESOURCES:** FEDERAL TRADE COMMISSION www.ftc.gov US Secret Service Field Offices www.usss.treas.gov/field_offices Electronic Crimes Task Force www.ectaskforce.org/regional_locations US Postal Inspection Service www.usps.com/postalinspectors E-Information Network www.einformation.usss.gov International Association of Chiefs of Police www.theiacp.org ID Safety Resources www.idsafety.org/enforcement/resources/ International Association of Financial Crimes Investigators www.iafci.org The Identity Theft Assistance Center (ITAC) www.identitytheftassistance.org National Crime Justice Reference Center www.ncjrs.org	

VICTIM ASSISTANCE - RESOURCES:

✓ the FTC maintains a COMPREHENSIVE WEB SITE devoted to identity theft: www.ftc.gov/IDTheft and includes:

→ information for victims/business and law enforcement;

→ *self-reporting* identity theft complaint process for victims of identity theft:
- ► does *NOT* replace/take the place of the reporting of identity theft incidents to law a enforcement agency;

→ consumer information on how to AVOID/DETECT identity crime;

→ what steps to take if an individual's identity is stolen;

✓ the FTC maintains an identity crime HOTLINE for victims at 1-877-IDTHEFT (1-877-438-4338) for victims to:

→ report identity theft for entry into the FTC database;

→ receive counseling from trained personnel to:

- ► resolve credit-related problems resulting from misuse of their identity;
- ► explain their rights under the Fair Credit Reporting Act and procedures to correct misinformation on their credit reports;
- ► explain the victim's responsibility for unauthorized charges on their credit card accounts;
- ► advice on their rights under the Fair Debt Collection Practices Act which describes debt collector practices;
- ► referral to the appropriate federal agency that has a program in place to assist consumers when investigation and resolution of the identity crime falls under the jurisdiction of that different agency:

  Example:

  ✶ Social Security Administration hotline for social security number misuse/fraud;

✓ the Identity Theft Resource Center is a non-profit organization that provides:
→ victim support;
→ consumer education;
- ► www.idtheftcenter.org

✓ the Privacy Rights Clearinghouse is a non-profit organization specializing in consumer education:
- ► www.privacyrights.org

(PPT SLIDES # 120-123)

Identify resources available to a crime victim.

Identify resources available to the victim for crimes involving identity theft/fraud.

Instructor Note:

The Federal Trade Commission, via its website, provides a variety of services to victims of identity theft. That site contains numerous informational brochures as well as sample letters to creditors. The FTC also provides a form for the self-reporting of identity theft crimes.

✓ **Maryland Attorney General's Office – ID Theft Unit:**
www.oag.state.md.us/idtheft

→ provides general information and assistance to victims of identity theft/fraud:
- ✶ ID Theft Unit – 410-576-6491:
  idtheft@oag.state.md.us
  - protect self from identity theft;
  - obtain a credit report;
  - freeze credit;
  - apply for/obtain an Identity Theft Passport;

→ provides an IDENTITY THEFT PASSPORT to victims of identity theft:
- ✶ requires victim to submit a ***written*** application to the Identity Theft Unit:
  - photocopy of Maryland Driver's License or State-issued Identification Card;
  - copy of the police report;
- ✶ background check made to verify victim's identity and details of the crime;

IDENTITY THEFT PASSPORT:

✓ in 2006, the Maryland Legislature enacted and the Governor signed into law CR § 8-305, entitled IDENTITY THEFT PASSPORTS, which have a twofold purpose to:

→ help an identity theft victim to resolve financial issues caused by the crime; and
→ prevent wrongful arrest if the victim's identity has been used by a suspect during the commission of a crime;

CR § 8-305:

(a) *Definitions.* – (1) In this section the following words have the meanings indicated.

(2) "Identity fraud" means a violation of § 8-301 of this subtitle.

(3) "IDENTITY THEFT PASSPORT" means a card or certificate issued by the Attorney General that verifies the identity of the person who is a victim of identity fraud.

(b) *In general.* – A PERSON WHO KNOWS OR REASONABLY SUSPECTS THAT THE PERSON IS A VICTIM OF IDENTITY FRAUD AND HAS FILED A REPORT UNDER § 8-304 OF THIS SUBTITLE MAY APPLY FOR AN IDENTITY THEFT PASSPORT THROUGH A LAW ENFORCEMENT AGENCY.

(PPT SLIDES # 124-127)

Instructor Note:

The Office of the Maryland Attorney General – ID Theft Unit is the main LOCAL entity that can provide assistance/information to Maryland residents who become victims of identity theft.

The ID Theft Unit can provide information about how to:
- protect self from identity theft;
- obtain a credit report;
- freeze credit;
- apply for and obtain an Identity Theft Passport;

(c) *Processing.* – A law enforcement agency that receives an application for an identity theft passport shall submit the application and a copy of the report filed under § 8-304 of this subtitle to the Attorney General for processing and issuance of an identity theft passport.

(d) Issuance. – (1) The Attorney General, in cooperation with a law enforcement agency, may issue an identity theft passport to a person who is a victim of identity fraud.

(2) The Attorney General may not issue an identity theft passport to a person before completing a background check on the person.

(e) *Use.* – A person who is issued an identity theft passport under subsection (d) of this section may present the identity theft passport to:

(1) A LAW ENFORCEMENT AGENCY TO HELP PREVENT THE ARREST OR DETENTION OF THE PERSON FOR AN OFFENSE COMMITTED BY ANOTHER USING THE PERSON'S PERSONAL IDENTIFYING INFORMATION; OR

(2) a creditor to aid in the investigation of:

(i) a fraudulent account that is opened in the person's name; or

(ii) a fraudulent charge that is made against the account of the person.

(f) *Acceptance or Rejection of passport.* – (1) A LAW ENFORCEMENT AGENCY or creditor THAT IS PRESENTED WITH AN IDENTITY THEFT PASSPORT UNDER SUBSECTION (e) OF THIS SECTION HAS *SOLE* DISCRETION TO ACCEPT OR REJECT THE IDENTITY THEFT PASSPORT.

(2) In determining whether to accept or reject the identity theft passport, THE LAW ENFORCEMENT AGENCY or creditor MAY CONSIDER THE SURROUNDING CIRCUMSTANCES AND AVAILABLE INFORMATION REGARDING THE OFFENSE OF IDENTITY FRAUD AGAINST THE PERSON.

(g) *Confidentiality.* – An application for an identity theft passport submitted under this section, including any supporting documentation:

(1) is NOT a public record; and

(2) may NOT be released except to a law enforcement agency in this or another state.

(h) *Regulations.* – The Attorney General shall adopt regulations to carry out the provisions of this section.

IDENTITY THEFT PREVENTION:

✓ the FTC web site offers a number of COMMONSENSE suggestions to consumers on steps to take to MINIMIZE the risk of identity crime:

PERSONAL IDENTIFYING INFORMATION:

→ NEVER reveal personal identifying information:
- ► over the PHONE;
- ► through the MAIL;
- ► on the INTERNET:
  - ✶ UNLESS *YOU* HAVE INITIATED CONTACT;
  - ✶ *KNOW* WHO YOU ARE DEALING WITH;
  - ✶ KNOW HOW THE INFORMATION WILL BE USED;

→ BEFORE sharing personal information CONFIRM that you are DEALING WITH A LEGITIMATE ORGANIZATION;

→ PROTECT YOUR SOCIAL SECURITY NUMBER:
- ► DO NOT CARRY IT IN YOUR WALLET/PURSE;
- ► STORE IT IN A SECURE PLACE;
- ► GIVE IT OUT ONLY WHEN ABSOLUTELY NECESSARY:
  - ✶ ask to use another identifier in its place;

FINANCIAL INFORMATION:

→ READ ALL BILLS/STATEMENTS ESPECIALLY CREDIT CARD BILLS CAREFULLY:
- ► DISPUTE WITH CREDITOR ANY CHARGES YOU DID NOT MAKE/AUTHORIZE;

→ ORDER a copy of your CREDIT REPORT EVERY YEAR from each of the major credit reporting agencies:
- ► VERIFY that the information is ACCURATE:
  - ✶ all consumers may receive a FREE credit report from www.annualcreditreport.com
    - ■ Maryland law provides for an annual free credit report on request;

→ obtain and MONITOR "specialty reports:"
- ► free upon request:
  - ✶ insurance claims history:
    - ■ 866-312-8076;
    - ■ www.personalreports.lexisnexis.com/index.jsp
- ► banking account history:
  - ■ 800-428-9623;
  - ■ www.consumerdebit.com
- ► public records report:
  - ■ www.personalreports.lexisnexis.com/index.jsp

(PPT SLIDES # 128-146)

Instructor Note:

Recommendations to prevent identity theft are included in this section as part of a comprehensive lesson plan on Identity Theft.

Enabling Objective:

Identify several different ways by which an individual can safeguard his/her personal identifying information.

The information provided has been compiled from a variety of different sources. It is not intended to be an all-inclusive list of recommendations.

Sources:
www.ftc.gov
www.privacyrights.org
www.trynova.org

(PPT SLIDE # 131)

→ **ACTIVELY MONITOR ACCOUNTS FOR SUSPICIOUS ACTIVITY:**
- ► **IMMEDIATELY CONTACT THE CREDIT COMPANY/FINANCIAL INSTITUTION WHEN UNAUTHORIZED ACTIVITY IS FOUND;**
- ► **FILE A POLICE REPORT IF USE IS FRAUDULENT;**
  - ✶ **43% of all reported identity fraud are spotted by victims during self-monitoring;**

PERSONAL CHECK CASHING:

(PPT SLIDE # 133)

→ **be aware of information-gathering when cashing a personal check:**
- ► **writing a credit card number on a personal check:**
  - ✶ **Maryland Law prohibits requesting or recording the account number of any credit card of the drawer on the check or other draft**
    - ■ **Consumer Protection Act - Title 13 Subtitle 3 – Unfair or Deceptive Practices § 13-318;**
  - ✶ **may ask drawer to display a credit card for identification/credit worthiness;**
  - ✶ **may record the type or issuer of the credit card;**
  - ✶ **record the account number/expiration date if the person has agreed with the credit card issuer to cash checks as service to the issuer's cardholders and the issuer has guaranteed payment of the cardholders checks cashed by that person;**

FINANCIAL PRIVACY:

(PPT SLIDE # 132)

→ **federal law requires banks/credit card companies/insurance companies and brokerage firms to send a privacy notice each year:**
- ► **companies that sell information to unaffiliated third parties must provide an OPT OUT provision:**
  - ✶ **PRIVACY NOTICE will contain either a form or toll-free telephone number to call;**

USE OF TOLL FREE TELEPHONE NUMBERS:

→ **avoid using 800/866/877/888/900 telephone numbers unless a relationship with company already exists:**
- ► **incoming calls can be recorded by an Automatic Number Identification system (ANI) and the telephone number sold to telemarketers for mail or phone solicitations:**
  - ✶ **FCC requires user permission prior to selling the phone number;**

USE OF CORDLESS AND CELLULAR PHONES:

→ cell phones emit a radio signal that can be captured by a radio scanner:
- ► newer DIGITAL models are less likely to be "intercepted;"
- ► care should be taken when giving personal identifying information over a cell phone in public;

MAIL:

→ HANDLE MAIL CAREFULLY:
- ► DEPOSIT OUTGOING MAIL IN POSTAL COLLECTION BOXES OR AT THE POST OFFICE:
  - ✶ not in unsecured mailboxes;
- ► PROMPTLY REMOVE MAIL FROM MAILBOX:
  - ✶ have mail held at the post office for pick up if not able to remove it from mailbox for any length of time;

→ TEAR UP/SHRED IMPORTANT PAPERWORK OR RECEIPTS WITH PERSONAL INDENTIFYING INFORMATION ON THEM PRIOR TO DISPOSING OF IN THE TRASH OR RECYCLABLES;

→ PRE-APPROVED CREDIT OFFERS:
- ► REMOVE NAME from mailing lists:
  - ✶ 888 – 5OPTOUT [888-567-8688;
  - ✶ www.optoutprescreen.com

→ USE OPT OUT to reduce "junk" mail:
- ► many mail order firms/magazines/credit card companies provide a box to check if individual does not want name/address/shopping habits to be sold/shared with other companies;
  - ✶ warranty and product registration cards;
  - ✶ joining/donating money to clubs/charities:
    - ■ inform them in writing not to sell/share name with other groups;

→ AVOID entering SWEEPSTAKES/other contests:
- ► entries are used to compile mailing lists for marketers/other solicitors;

(PPT SLIDE # 138)

COMPUTER:

(PPT SLIDE # 139)

- → LOCK COMPUTERS WHEN NOT IN USE;
- → INSTALL/UPDATE COMPUTER VIRUS PROTECTION SOFTWARE REGULARLY;
- → no "one thing" makes a computer/data secure;
- → MAINTAIN/UPDATE SECURITY as frequently as possible;
- → KEEP COMPUTER UPDATED:
  - ► use automatic updates;
- → use a virus scan and anti-spyware software:
  - ► use automatic updates;
  - ► set virus scan to CD, DVD and USB automatically;
- → do not send personal information to unsecured websites:
  - ► look for "https" which indicates secure site:
    - • unless so marked assume not encrypted;
- → wipe computer hard drive before donating/selling or trashing computer:
  - ► according to a 2009 survey 40% of hard drives sold on E-Bay contained sensitive personal identifying information
  - ► use a utilities program:
    - • free download:
      - ▪ www.killdisk.com
  - ► physically destroy hard drive:
    - • caution to be used to avoid harmful chemicals;

PASSWORDS/PINS:

(PPT SLIDE # 140)

- → CREATE A "STRONG" PASSWORD:
  - ► one that is NOT 'GUESSABLE;"
  - ► the longer a password is the harder it is to decode;
- → do NOT use personal identifying information in passwords:
  - ► birth date;
  - ► name/initials;
  - ► other personal identifiers;
- → do NOT maintain/store written passwords near where computer is stored;
- → CHANGE passwords frequently if possible;
- → do NOT use same password for multiple accounts/services;
- → use password "keeper" security software to store passwords;

EMAIL/FILE SHARING: (PPT SLIDE # 141)

→ do ***NOT*** :
- ► OPEN COMPUTER FILES/ATTACHMENTS/LINKS SENT BY STRANGERS;
- ► OPEN HYPERLINKS;
- ► DOWN LOAD PROGRAMS:
  - ✶ FROM PEOPLE/COMPANIES THAT YOU DO ***NOT*** KNOW;

→ AVOID SENDING PERSONAL IDENTIFYING INFORMATION IN EMAIL/TEXT MESSAGES/SOCIAL NETWORKING SITES;

→ be CAUTIOUS ABOUT USING FILE SHARING PROGRAMS which can capture passwords or other information when they are typed into computer by user;

→ AVOID USING FREE FILE SHARING PROGRAMS for music/movies/other entertainment purposes;

→ ENSURE INTERNET SITES ARE SECURE ***BEFORE*** SUPPLYING PERSONAL OR FINANCIAL INFORMATION ONLINE;

→ do ***NOT*** SHARE PASSWORDS OR OTHER ACCOUNT INFORMATION;

→ USE DISCRETION WHEN SHARING PERSONAL IDENTIFYING INFORMATION ON E-COMMERCE SITES;

→ USE DISCRETION WHEN PUBLISHING INFORMATION ON SOCIAL MEDIA WEBSITES:
- ► monitor the personal information that children or other family members are posting on social sites;

→ do NOT ACCESS SECURE WEB SITES WHEN USING PUBLIC Wi-Fi;

SOCIAL NETWORKING WEBSITES: (PPT SLIDE # 142)

→ do NOT post any information/photographs that you would not want accessible to the world;

→ use caution when clicking on "links" or installing "apps;"

→ be aware of any pleas for financial assistance:
- ► verify any requests for financial assistance;

INSTANT MESSAGING: (PPT SLIDE # 142)

→ most information sent is not encrypted:
- ► do NOT send personal identifying information via IM;

HAND HELD DEVICES: (PPT SLIDE # 143)

→ **ENSURE DEVICES LOCK AUTOMATICALLY AFTER A MAXIMUM OF 15 MINUTES IDLE TIME;**

→ enable device to "wipe" information after a predetermined number of invalid password attempts;

WIFI:

→ many public WiFi "hotspots" are NOT secure;
- ► information "flies" through the air and can be intercepted and compromised;

USE OF CREDIT CARD ON THE INTERNET: (PPT SLIDE # 143)

→ **use a credit card only if your browser identifies the website as a SECURE CONNECTION;**
- ► ADDRESS BAR SHOULD READ **"https;"**

→ if a victim is notified that his/her private records were involved in a data breach:
1) confirm that the letter is LEGITIMATE;
2) take advantage of any free protection services that are offered;
3) **PLACE A FRAUD ALERT ON CREDIT REPORT:**
   - ► a FRAUD ALERT requires lenders to make sure that it is actually the victim who is applying for credit;

TELEMARKETERS: (PPT SLIDE # 144)

→ LIMIT calls from telemarketers:
- ► "DO NOT CALL REGISTRY:"
  - ✶ 888 -382 – 1222;
  - ✶ www.donotcall.gov
- ► FCC regulations currently prohibit telemarketers from using automated dialers to call cell phone numbers:
  - ✶ DO NOT CALL REGISTRY will accept cell phone numbers;
- ► look for/use "opt out" instructions on "junk" faxes;

DATA MINING:

(PPT SLIDE # 145)

- ✓ definition:
  - → practice of:
    - ► collecting "bits" of data including personal identifiers/information from variety of sources:
      - ✶ use "tracking" device to identify individual's web site visits/usage:
        - ● user/consumer "gps;"
    - ► compiling that information into "portrait" of that individual;
    - ► selling /sharing that "portrait" to businesses:
      - ✶ advertising then directed at individual either online or via mail;
      - ✶ collected data can also be accessed by prospective employers;

- ✓ sources of collected data include but are not limited to:
  - ► e-commerce transactions;
  - ► online searches;
  - ► social networking sites:
    - ✶ web sites visited;
  - ► customer "reward" cards;
  - ► product warranty/extended service cards;
  - ► cell phone "apps" use;
  - ► consumer surveys;
  - ► public records;
  - ► other businesses;

- ✓ seen by some as invasion of privacy;

- ✓ currently legal practice:
  - → congressional hearings underway looking into the practice:
    - ► considering "opt-out" provision similar to "Do Not Call Registry;"

- ✓ disclaimer regarding privacy issues/information sharing usually included on web site/billing statements;

- ✓ no way to correct misinformation that has been collected/compiled/distributed which can affect various life transactions such as obtaining:
  - ► credit;
  - ► employment;
  - ► health/life insurance;

"VISHING:" → a technique for stealing personal identifying information using the telephone: ► similar to "phising" – an online scam intended to obtain personal information via the computer; → using voice over technology identity thief makes a phone call appear to come from a legitimate source (phone number) even when the recipient has caller ID: ► recipients of calls should be suspicious when receiving calls asking for credit card numbers/bank accounts/Social Security number/PIN numbers: ✶ VERIFY legitimacy of the call by contacting the company directly BEFORE providing information: ▪ USE ONLY A KNOWN LEGITIMATE NUMBER such as the one that appears on the reverse side of a credit card or one that has been furnished by the company in question; **MEDICAL RECORDS/HISTORY:** → determine if medical history is stored on an insurance data base: ► request free copy of medical history – 1x per year; ► Medical Information Bureau (MIB): ✶ www.mib.com/html/request_your_record ► request a copy of medical file from health care provider(s): ✶ HIPAA provides individuals the right to access their medical records; ► read health care providers privacy notices;	(PPT SLIDE # 144) (PPT SLIDE # 146)

AVAILABLE VICTIM RESOURCES: **The following represent a few of the resources available to the victims of identity theft:** **The Federal Trade Commission** **www.ftc.gov** **Identity Theft Assistance Center (ITAC)** **www.identitytheftassistance.org** **National Organization for Victim Assistance** **www.trynova.org** **Office of Maryland Attorney General** **www.idtheft@oag.state.md.us** **Internet Crime Complaint Center (US)** **www.ic3.gov** **National Crime Prevention Council** **www.ncpc.org** **Privacy Rights Clearinghouse** **www.privacyrights.org** **Scam Victims United** **www.scamvictimsunited.com**	**(PPT SLIDE # 123)** **Instructor Note:** **The referenced organizations and websites are available to victims of identity theft. The list is not all-inclusive nor is a website's inclusion in this list an endorsement of use.**

SUMMARY

(PPT SLIDE # 148)

1. DETER – DETECT – DEFEND – AVOID IDENTITY THEFT.

2. WHEN ASKED FOR PERSONAL IDENTIFYING INFORMATION:
   - → VERIFY THE REQUEST AS COMING FROM A LEGITIMATE ENTITY;
   - → QUESTION THE NEED FOR AND PURPOSE FOR THE INFORMATION:
     - * ASK HOW THE INFORMATION WILL BE USED;
   - → ASK IF THERE IS A WRITTEN POLICY REGARDING THE REQUEST FOR THE INFORMATION:
     - * ASK TO SEE IT/HAVE A COPY SENT TO YOU;
   - → ASK "HOW" THE INFORMATION WILL BE SAFEGUARDED FROM UNAUTHORIZED ACCESS PRIOR TO GIVING IT:
     - * ASK WHO WILL SEE/HAVE ACCESS TO THE INFORMATION;
   - → REVIEW ALL PRIVACY NOTICES SENT BY COMPANIES WITH WHOM YOU ARE DOING BUSINESS;
   - → ASK HOW THE RECORDS WILL BE DISCARDED WHEN THEY ARE NO LONGER NEEDED;
   - → GIVE ONLY THE MINIMUM AMOUNT OF INFORMATION;
   - → TAKE ADVANTAGE OF ANY AVAILABLE "OPT OUT" OPPORTUNITIES;
   - → IF NOT SATISFIED WITH THE RESPONSES GIVEN ASK TO SPEAK TO A SUPERVISOR OR TAKE YOUR BUSINESS ELSEWHERE.

3. AN INDIVIDUAL IS BEST ADVOCATE FOR HIS/HER PRIVACY RIGHTS.

4. IF IDENTITY THEFT/FRAUD OCCURS:
   - → IMMEDIATELY REPORT ANY IDENTITY THEFT TO THE POLICE.
   - → MAINTAIN A *WRITTEN* LOG OF EVERYTHING THAT IS DONE AND EVERY PERSON CONTACED IN THE RECOVERY PROCESS:
     - * INCLUDE TIME SPENT/EXPENSES INCURRED.
   - → RETAIN COPIES OF ALL DOCUMENTS USED IN THE RECOVERY PROCESS IN A SAFE PLACE.
   - → FOLLOW-UP ALL TELEPHONE CONVERSATIONS WITH A LETTER USING CERTIFIED MAIL – RETURN RECEIPT REQUESTED.

PRESENTATION GUIDE	TRAINER NOTES
EVALUATION/CLOSURE: **1. Identity theft is best defined as:** a. only crimes identified by the Federal Trade Commission involving a theft of services using a computer. **b. the illegal use of another person's personal identifying information in order to gain something of value or to facilitate criminal activity.** c. the authorized use of another individual's PIN to conduct a business transaction. d. only theft crimes involving the use of another person's personal identifying information as counted by the FBI in the Uniform Crime Reporting (UCR) system. **2. Under Maryland Law [CR § 8-301] which of the following is NOT considered to an example of a personal identifier:** a. an individual's date of birth; b. an individual's mother's maiden name; **c. an individual's place of birth;** d. an individual's financial account number; **3. Under Maryland Law [CR § 8-301] which of the following is NOT an element of the crime of Identity Fraud:** a. using another's personal identifying information without the person's consent. b. knowingly, willfully and with fraudulent intent possessing, obtaining or helping another to gain possession of another person's personal identifying information. c. using, selling or transfer the personal identifying information of another person to obtain goods or services. **d. Identity Fraud only applies to the use of another's personal identifying information when it is fraudulently obtained by way of electronic means.**	**TERMINAL OBJECTIVE:** **Given various criminal situations demonstrate the ability to identify elements of a given crime utilizing the Annotated Code of Maryland and/or the Digest of Criminal Laws, that enable an officer to make a warrant-less arrest.** **ENABLING OBJECTIVES:** Define the term IDENTITY THEFT. Identify the basic elements of the crime of identity theft/fraud as contained in the Annotated Code of Maryland.

4. **One resource available to the citizens of Maryland in cases of identity theft/fraud is which of the following:**

   a. Federal Trade Commission.
   b. Office of the Solicitor General – Consumer Affairs Unit.
   c. Office of the Special Prosecutor.
   d. Public Defenders office.

5. **As per Maryland Law – CR § 8-305 - the office of the Maryland Attorney General processes applications by victims of identity theft/fraud for which of the following:**

   a. amended driver's license.
   b. credit monitoring report.
   c. Identity Theft Passport.
   d. Identity Theft Affidavit.

6. **Under Maryland Law, § 8-304, one of the stated uses of the Identity Passport issued by the Office of the Maryland Attorney General is that it be used by an individual:**
   a. if confronted by a creditor to show that the individual has had his/her identity compromised;
   b. in place of a Maryland Driver's license by an individual who has had his/her identity compromised.
   c. whenever the individual conducts a financial transaction;
   d. to help prevent the arrest or detention for an offense committed by another person who has used the individual's personal identifying information.

7. **In addition to contacting a local law enforcement agency and filing a report an individual who has had his/her identity stolen/compromised should make a report to:**

   a. the Federal Trade Commission;
   b. the Department of Justice;
   c. the Federal Securities and Exchange Commission;
   d. the Internal Revenue Service;

8. **The following is <u>NOT</u> a resource that can provide information or assistance to a victim of identity theft:**

   a. the Office of the Maryland Attorney General.
   b. the Federal Trade Commission.
   c. the Privacy Rights Clearinghouse.
   d. the Electronic Transaction Enforcement Unit.

<u>TERMINAL OBJECTIVE:</u>

Identify resources available to a crime victim.

<u>ENABLING OBJECTIVE:</u>

Identify resources available to the victim for crimes involving identity theft/fraud.

9. Under Maryland Law – CR § 8-304 allows an individual to report the crime of identity theft/fraud under the following circumstances: a. only when the crime has occurred in the jurisdiction of the officer taking the report. **b. when either the crime has occurred in the county in which the individual lives or the individual is reporting the crime in the jurisdiction in which it occurred.** c. only when the individual is a resident of the State of Maryland. d. only when the value of the goods or services received as a result of the identity theft exceeds $500. **10. Under Maryland Law – CR § 8-304 - once an officer has taken a report from a victim of identity theft the law enforcement agency is to:** **a. provide a copy of the report to the victim.** b. provide a copy of the report to the Office of the Maryland Attorney General. c. provide a copy of the report to the Internal Revenue Service. d. provide a copy of the report to any financial institution/company mentioned in the report. **11. When taking a report of identity theft/fraud from a victim it is highly recommended that the officer taking the report:** a. refer the victim to an attorney who specializes in consumer protection cases. b. recommend that the victim take no action until contacted by an investigator from the Federal Trade Commission. **c. recommend that the victim maintain a written log of all actions taken when attempting to resolve his/her identity theft including the names of persons contacted during this process.** d. recommend that the victim file an Identity Theft Affidavit with the Internal Revenue Service; **12. The following is <u>NOT</u> a potential resource available to an officer investigating the crime of identity theft/fraud:** a. the Federal Trade Commission. b. the United States Postal Inspection Service. c. the Office of the Maryland Attorney General. **d. the United States Bureau of Credit Monitoring.**	**<u>TERMINAL OBJECTIVE:</u>** **Demonstrate completion of acceptable police reports for various offenses, incidents, or situations.** **<u>ENABLING OBJECTIVE:</u>** Apply the law as contained in the Annotated Code of Maryland that requires a law enforcement officer to prepare and file a report from the victim of identity/theft/fraud. **<u>TERMINAL OBJECTIVE:</u>** **Identify the basic responsibility of the officer when Investigating the crime of identity theft.** **<u>TERMINAL OBJECTIVE:</u>** **Identify the resources available to an officer while conducting a criminal investigation.** **<u>ENABLING OBJECTIVE:</u>** Identify the resources available to the officer for crimes involving identity theft/fraud.

13. The Federal Trade Commission provides all of the following to law enforcement officers EXCEPT:

a. access to the Consumer Sentinel Program.
b. funding to investigate incidents of identity theft.
c. resource information regarding the crime of identity theft/fraud.
d. victim assistance information that an officer can supply to an identity theft victim.

14. All of the following are true about the Consumer Sentinel Program developed by the Federal Trade Commission EXCEPT:

a. it is a database containing complaints from victims of identity theft/fraud available to law enforcement officers.
b. it contains reports of recent identity theft schemes.
c. provides e-mail updates to law enforcement when identity theft trends/schemes are entered by allied law enforcement agencies.
d. provides an application by which law enforcement agencies can apply for a grant to investigate identity theft crimes.

15. Which of the following is NOT an example of personal identifying information that is most likely to be stolen or compromised:

a. financial account access codes or passwords.
b. work computer passwords.
c. medical or educational records.
d. a gift card from a local business.

16. The statement "it is not a matter of IF an individual's personal identifying information will be compromised but only a matter of WHEN that information will be compromised" is accurate because of all of the following EXCEPT:

a. Items of personal identifying information are contained in many documents/records that are readily available to the public.
b. The public has only recently taken the threat of identity theft/compromise as a serious issue.
c. Many individuals fail to take the minimum precautions to safeguard their identity such as shredding their discarded financial statements or pre-approved credit offers.
d. Computer software is now so secure that it is impossible for unauthorized individuals to access personal information stored on most personal and work computers.

TERMINAL OBJECTIVE:

Define crime prevention.

ENABLING OBJECTIVES:

Identify several types of personal and/or financial information that may be stolen or compromised to include, at a minimum:

- personal identifiers:
  - name;
  - date of birth;
  - address;
  - mother's maiden name;
- credit, debit, checking, savings, other existing financial accounts;
- account access codes/passwords;
- social security number;
- medical records;
- driver's license number/identification number;
- educational background and records; and
- computer passwords.

17. When providing citizens with crime prevention tips dealing with identity theft an officer should point out all of the following <u>EXCEPT</u>:

a. most identity thefts/compromises are committed by individuals who are known to the victim such as family members, friends or co-workers.
b. improperly discarded mail such as pre-approved credit offers and old financial statements whether as trash or when re-cycling can be easy targets for an identity thief.
c. individuals should always ask individuals seeking personal information as part of a requirement for medical treatment what the personal information is needed for and how will it be safeguarded.
d. financial statements and billing statements should be reviewed for discrepancies as soon as they are received and any discrepancy should be reported immediately to the financial institution or company.

18. Identify which of the following statements is <u>NOT</u> true:

a. a child's educational records contain personal identifying information that can be used to establish a fraudulent identity.
b. children under the age of 12 years can not be the victim of identity theft because he/she has no credit history.
c. a child's medical records, if not properly safeguarded by a health care provider, can be compromised by an identity thief.
d. a child's birth certificate contains unique personal identifiers that can be useful to an identity thief.

19. Which of the following statements is <u>FALSE</u>:

a. Social networking websites can be exploited by individuals who attempt to gather personal identifying information.
b. When an individual shares personal information on a social networking website that information almost always becomes public unless the individual restricts access to it.
c. A social networking website can change its privacy policy at any time without the user's permission.
d. Individuals who are approved to visit a user's "site" will never re-post an individual's personal identifying information because they realize that it may be fraudulently used by someone else.

Identify several different ways in which personal information including financial information may be stolen/compromised, to include at a minimum:

- the use of home computers;
- discarded/stolen mail;
- discarded personal and/or financial records; and
- theft/compromise during *<u>legitimate</u>* use of information by victim during a third party transaction.

20. Which of the following statements is <u>FALSE</u>: a. Government records such as professional licenses and property tax records are documents that can be easily compromised by an identity thief. b. Examples of public records are documents such as marriage certificates, court records, birth certificates and death certificates. **c. When attempting to view a public record such as a birth certificate an individual <u>normally</u> has to produce more than a photo id as identification before being allowed to view the document.** d. Virtually every major change in life is recorded somewhere in a government document.	
21. Identity thieves are <u>least</u> likely to use another individual's stolen or compromised personal information to: a. obtain medical treatment. b. obtain financial assistance in the form of a loan. c. avoid arrest and prosecution for a crime. **d. all of the examples presented are likely uses of another's personal identifying information by an identity thief.**	Identify several examples of the crime of identity theft/fraud to include, at a minimum, the theft/fraudulent use of: ▪ existing credit/debit cards/financial accounts; ▪ other financial records and personal financial information to obtain credit or other financial assistance; ▪ personal information to obtain various services such as medical treatment, government and social services, educational assistance, etc; and ▪ personal information to obtain government identity cards, licenses or other official documents.
22. Maryland Law – CR § 8 – 302 <u>prohibits</u> an individual from selling/offering for sale/offer to issue an identification card/document all of the following <u>EXCEPT</u> an identification card or document which: a. has a blank space for a person's age/date of birth. b. contains a person's incorrect age/date of birth. c. contains the incorrect name of the person. **d. contains a physical description of the person to include the person's height, weight and hair color.**	
23. Under Maryland Law – CR § 8-303 – a government identification document includes all of the following <u>EXCEPT</u>: a. passport. b. adoption decree. c. alien registration card. **d. alumni card from an accredited college/university.**	

24. All of the following are steps an individual can take to safeguard his/her identity when using a personal computer <u>EXCEPT</u>: **a. send personal information via the Internet when using a laptop computer that is connected to the Internet by public access wi-fi;** b. lock a workplace computer when not in use; c. send personal identifying information over a secured Internet website that is marked with an "S" in the address bar – https: d. physically destroy a hard drive when disposing or re-cycling a computer; **25. All of the following are common security errors that many individuals make when sending or receiving email <u>EXCEPT</u>:** a. down loading free programs from unknown sources. b. including personal identifying information in emails. **c. using caution and discretion when publishing any type of personal information on a social network.** d. using free file sharing programs for entertainment purposes even when sent by known sources. **26. Which of the following statements is <u>FALSE</u> regarding steps that can be taken to prevent identity theft:** a. periodically obtain and review your credit report. b. ensure that electronic handheld devices such as blackberries/iphones etc. are automatically locked after 15 minutes of nonuse/inactivity. c. ask your health care provider how he/she will safeguard your personal identifying information which is supplied as a prerequisite for treatment. **d. ignore the privacy statements that routinely accompany credit card statements/other financial statements.**	Identify several different ways by which an individual can safeguard his/her personal identifying information.