Directions

- Read all the directions for each question carefully and think about the answer.

- This Assesslet contains five items. Questions 1-3 are selected-response items where you choose the one BEST answer. Answer each question by filling in the circle on your answer document.

- Question 4 is a constructed-response item. Write your answer on the lines provided on your answer document.

- Question 5 is an extended-response item. Use the scratch paper provided to plan your writing. Then, write your essay on the lines provided on your answer document.

- Be sure to write your answers in the spaces provided on the answer document.
Read Passages A and B. Then, respond to the questions that follow.

Passage A: An Excerpt from The United States Department of Justice

"But he that filches from me my good name/Robs me of that which not enriches him/and makes me poor indeed."
- Shakespeare, Othello, act iii. Sc. 3.

What is Identity Theft?

The short answer is that identity theft is a crime. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for economic gain.... Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data — especially your Social Security number, your bank account or credit card number, your telephone calling card number, and other valuable identifying data — can be used, if they fall into the wrong hands, to personally profit at your expense. In the United States and Canada, for example, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts, or, in the worst cases, taken over their identities altogether, running up vast debts and committing crimes while using the victims’ names. In many cases, a victim’s losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his reputation in the community and correcting erroneous information for which the criminal is responsible.

In one notorious case of identity theft, the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim’s name, but called his victim to taunt him -- saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time -- before filing for bankruptcy, also in the victim’s name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused. This case, and others like it, prompted Congress in 1998 to create a new federal offense of identity theft.

Passage A continued on page 3
Many people do not realize how easily criminals can obtain our personal data without having to break into our homes. In public places, for example, criminals may engage in “shoulder surfing” or watching you from a nearby location as you punch in your telephone calling card number or credit card number, or listen in on your conversation if you give your credit card number over the telephone to a hotel or rental car company.

If you receive applications for “pre-approved” credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. (Some credit card companies, when sending credit cards, have adopted security measures that allow a card recipient to activate the card only from his or her home telephone number but this is not yet a universal practice.) Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.

In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information. In their haste to explore the exciting features of the Internet, many people respond to “spam,” unsolicited email that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data.

With enough identifying information about an individual, a criminal can take over that individual’s identity to conduct a wide range of crimes: for example, false applications for loans and credit cards, fraudulent withdrawals from bank accounts, fraudulent use of telephone calling cards, or obtaining other goods or privileges which the criminal might be denied if he were to use his real name. If the criminal takes steps to ensure that bills for the falsely obtained credit cards, or bank statements showing the unauthorized withdrawals are sent to an address other than the victim’s, the victim may not become aware of what is happening until the criminal has already inflicted substantial damage on the victim’s assets, credit, and reputation.

What’s the Department of Justice Doing About Identity Theft and Fraud?

The Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. In the fall of 1998, for example, Congress passed the Identity Theft and Assumption Deterrence Act. This legislation created a new offense of identity theft, which prohibits “knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or
to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.”

To victims of identity theft and fraud, the task of correcting incorrect information about their financial or personal status, and trying to restore their good names and reputations, may seem as daunting as trying to solve a puzzle in which some of the pieces are missing and other pieces no longer fit as they once did. Unfortunately, the damage that criminals do in stealing another person’s identity and using it to commit fraud often takes far longer to undo than it took the criminal to commit the crimes.

**What Should I Do If I’ve Become a Victim of Identity Theft?**

If you think you’ve become a victim of identity theft or fraud, act immediately to minimize the damage to your personal funds and financial accounts, as well as your reputation. Here’s a list - based in part on a checklist prepared by the California Public Interest Research Group (CalPIRG) and the Privacy Rights Clearinghouse - of some actions that you should take right away:

1. Contact the Federal Trade Commission (FTC) to report the situation, whether online,

2. By telephone toll-free at 1-877-ID THEFT (877-438-4338) or TDD at 1-866-653-4261, or

3. By mail to Consumer Response Center, FTC, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.

You may also need to contact other agencies for other types of identity theft:

1. Your local office of the Postal Inspection Service if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity;

2. The Social Security Administration if you suspect that your Social Security number is being fraudulently used (call 800-269-0271 to report the fraud);

3. The Internal Revenue Service if you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).

Call the fraud units of the three principal credit reporting companies: Equifax, Experian, and TransUnion.

*Passage A continued on page 5*
Contact all creditors with whom your name or identifying data have been fraudulently used. For example, you may need to contact your long-distance telephone company if your long-distance calling card has been stolen or you find fraudulent charges on your bill.

Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge. You may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).

**What Should I Do To Avoid Becoming a Victim of Identity Theft?**

To reduce or minimize the risk of becoming a victim of identity theft or fraud, there are some basic steps you can take. For starters, just remember the word “**SAM**”:

- **S** - Be *stingy* about giving out your personal information to others unless you have a reason to trust them, regardless of where you are.
- **A** - *Ask* periodically for a copy of your credit report.
- **M** - *Maintain* careful records of your banking and financial accounts.

Even if you take all of these steps, however, it’s still possible that you can become a victim of identity theft. Records containing your personal data -- credit card receipts or car rental agreements, for example -- may be found by or shared with someone who decides to use your data for fraudulent purposes.

*Excerpt from Public Domain: The U. S. Department of Justice*
Passage B: Identity Theft and Social Media

Growing up, most of us were likely taught not to speak to strangers, not to give out our names and addresses to people we didn’t know, or in general, to keep personal information to ourselves. But today, people have profiles on social media sites, smart phones capture our daily movements using GPS signals, and information about almost anyone can be found by just Googling a name on the internet. Is it no wonder that identity theft has become a major concern of people all over the world today and a growing area of crime?

In 2012, the Federal Trade Commission reported that more than 360,000 complaints of identity theft were registered. In 2014, Georgia ranked second per capita in reporting identity theft complaints. These complaints included everything from being asked to visit a scam website in an email to being the target of identity theft. Identity thieves are continuously finding new avenues to steal personal information.

One of the ways identity thieves gain information is via social media sites. With only limited information in the profile (name, place of birth, and year), a thief has ample information to steal a person’s identity. Doing a status update, however innocent this may seem, can leave you open to a variety of crimes. Making the statement that you are going away for the week on vacation alerts a criminal that your home will be vacant. It can also make an identity thief aware that your bank account may be accessed from remote locations via your phone or a public computer.

While people are becoming savvier about protecting themselves, many people are not aware that some sites ask for sensitive information that could be used in inappropriate ways to either steal your identity or to use your identity to commit crimes in malicious ways. The following information is often included in your profile, or is disclosed in conversations on social media sites:

- Your full name, including your middle name
- Your date of birth, which is often required
- Your home town
- Your relationship status
- The schools you attended and/or graduated from
- Your pet’s name
- Your religious affiliations, hobbies, clubs, etc.

Passage B continued on page 7
Who are those most susceptible to identity theft? Statistics from the Federal Trade Commission show that the group with the highest percentage of identity theft victims are aged 20-29. Some of the reasons for this seem to be that this group of people is less likely to keep a regular check on their bank accounts and credit card activity. The records indicate that they are also less careful when sharing information on social media.

In 2011, a Carnegie Mellon study of more than 40,000 children reported that children under the age of 18 were twice as often victims of identity theft as their parents. Teens are often less cautious about protecting their personal information. Teens often share personal information via sites such as Facebook, Twitter, and Instagram. The information shared often includes hints to things that a person might use to answer security questions for secure sites. Teens often have unused social security numbers. Thieves might sell the social security number to illegal immigrants so that they can obtain a fake ID for employment. Teens are also less cautious about sharing a credit card number with a friend to buy tickets for a concert or when they go out to eat. If the friend writes down the number and is not careful about destroying it, the number can be compromised. When teens use Wi-Fi, it is easy for a thief to obtain personal information. Smart phones store and transmit personal data. If the phone is lost, the information can be retrieved and used for malicious purposes. Importantly, teens often don’t understand the ramifications of identity theft and often consider themselves ‘immune’ to being a target. The impact identity theft has on things like applying for college scholarships, buying your first car, getting your first job, or your first place to live could be an obstacle that could take years to overcome.

An example of a teen who was caught up in identity theft turmoil:
I found myself sitting in an attorney’s office with my parents, waiting to meet with someone who I hoped could help me. Someone has stolen my identity and I am trying to get into college. When my college loan application was rejected, I found out information that led me to the conclusion that someone was using my personal information. I need help!

Apparently, someone had stolen my social security number and has been using it for a while. I lost my wallet a couple years ago, but I never reported my social security card as stolen. I also filled out all the information in the Profile on Facebook and used my phone to make purchases all the time. I had no idea when or how the person had connected my information, but this unknown thief has created a lot of problems for me. Once I started investigating, with my parents help, we found that the person had applied for credit cards in my name, bought a car, and some furniture. I had contacted the credit card companies, but I have to go through some type of legal process to prove that I am really me and that I am not the one who ran up all those bills.

Passage B continued on page 8
Once we talked to the attorney, we realized that it was going to take some time...and cost some money...to try to clear my name and set things straight. He worked really hard to help me talk to the college loan offices so that I could apply for loans to go to school. It took an extra year before the matter had been resolved to the point that I could get the loan, and I was finally able to start school. The attorney is still working to clear up the credit card debt. What a way to start my life after graduation!

How do we prevent becoming victims of identity theft? Just a couple of easy steps can help when using social media sites. These will not protect against all identity theft, but will be a good place for everyone to start to be proactive and responsible.

- Use different passwords for every site you use.
- Don’t share passwords with anyone.
- Use a password to access your phone.
- Keep track of credit card and bank statements regularly.
- Use credit protection services if you can to monitor your accounts.
- Shred all mail that has any identifying information on it instead of discarding it in the trash.

Be responsible and protect your identity. There should be only one you!
Selected-Response Questions

For questions 1-3, answer each question by filling in the circle on your answer document.

1 What is the central idea of Passages A and B?
   A Identity theft is less today than ten years ago.
   B Identity theft is the biggest crime in the world today.
   C Identity theft is a growing problem and can affect anyone.
   D You need legal help if you’ve been a victim of identity theft.

2 In Passage A, which statement BEST supports a reason that identity theft has become more of a problem in the world today?
   A With enough identifying information about an individual, a criminal can take over that individual’s identity to conduct a wide range of crimes.
   B In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information.
   C The Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes.
   D Many people do not realize how easily criminals can obtain our personal data without having to break into our homes.

3 In Passage B, which statement BEST supports why the highest percentage of people ages 20-29 are most often the victims of identity theft?
   A This age group owns and uses the most smart phones.
   B This age group spends the most time using social media networks.
   C This group does not check their bank accounts and credit card activity regularly.
   D This age group does not create and use appropriate passwords for phone and Internet accounts.
Constructed-Response Question

4 Both of the passages discuss the problem of identity theft. Citing at least one example or detail from each passage, describe why you think identity theft is a threat to teenagers in your school.

Write your answer on the lines provided on your answer document.
Extended-Response Question

Identity theft impacts a person’s life in many ways. Citing examples from BOTH Passages A and B, discuss the impact that having your identity stolen could have on your life. What changes do you need to make in your daily activities to help prevent having your identity stolen? Use examples from the passages to support your thoughts.

Use the scratch paper provided to plan your writing. Then, write your essay on the lines provided on your answer document.