Data and Privacy Issues

Directions: Go to Quia.com and locate the quiz ***PF 7.03 Identity Theft Worksheet*** and answer the questions utilizing the information from this handout.

* Many businesses have legitimate reasons for obtaining personal information
* Financial institutions
* Health care providers
* Insurance companies
* Other businesses use personal information, such as your name, address, credit card number, and information about purchasing preferences and patterns for other purposes
* Process orders
* Market goods and services based on preferences
* Sell to other businesses
* Analyze to better understand consumer preferences and purchasing patterns
* Some websites use online profiling
* Companies collect information about the websites a consumer visits
* Information is used to predict what the consumer may buy in the future
* Cookies, or small files stored on a computer, enable a website to “remember” information about a visitor
* Security of websites
* Be cautious when surfing the Web
* Secure sites use safeguards to protect information from theft during certain types of transmissions
* Web addresses of secure sites begin with either “shttp://” or “https://”
* Social Security number
* Unique nine-digit number used by Social Security Administration to track one’s earnings
* An important piece of personal information
* Can be used to access bank and credit card accounts and other personal information
* Avoid carrying number or card in one’s wallet
* Do not print number on checks
* When businesses request Social Security number during routine transactions to identify you, ask how it will be used and avoid giving out number

Appendix 7.03F

**Tips for Protecting Yourself against Identity Theft**

The following are tips for protecting your personal information and to protect against identity theft:

* Order a copy of your credit report from each of the three credit reporting agencies every 12 months to monitor the information.
* Carry only the credit cards you really need and use.
* Make photocopies of the front and back of all cards in your wallet. This will be helpful in the event that your wallet is lost or stolen.
* Keep a list of your credit cards with account numbers, expiration dates, and toll-free numbers. You will need this information in case of loss or theft. This is also true of checking, savings, and investment accounts.
* Handle your mail with care. Deposit outgoing mail in post office boxes or at the post office. Promptly remove your mail from your mailbox once it is delivered.
* Keep items with personal information in a safe place, such as a locked drawer. Ask your home Internet provider about its security measures. Find out what measures you should take to protect your computer and its data.
* Keep a list of your credit cards with account numbers, expiration dates, and toll-free numbers. You will need this information in case of loss or theft. This is also true of checking, savings, and investment accounts.
* Safeguard sensitive information on your computer or online with passwords that include both numbers and letters. Avoid easily guessed combinations, such as your birthday. Don’t share your passwords, and don’t write them down where others can see them. Keep items with personal information in a safe place, such as a locked drawer.
* Before sending sensitive information on the Web, be sure it’s a secure site. Sites that have Web addresses that begin with either “shttp://” or “https://” are secure.
* Ask your home Internet provider about its security measures. Find out what measures you should take to protect your computer and its data.
* Tear or shred charge receipts, credit applications, and all financial statements. Cut or shred expired credit cards.
* Don’t carry your social security card or have the number printed on your driver’s license.
* Don’t throw away credit card receipts, monthly statements, or anything else with an account number on it without first shredding them.
* Don’t give your social security or bank account numbers to anyone without knowing the information will be secure and that the request for the information is necessary and authentic.
* Don’t give out personal information over the phone, through the mail, or by email, or on the Web unless you initiated the contact or are otherwise certain that the recipient is legitimate.
* Keep copies of the front and backsides of your credit cards. Store copies in a safe place separate from your cards.
* Don’t give your credit card number to just anyone. Know to whom you are giving the card to and how that the reason is legitimate.
* If you give your credit card to someone, make sure to it is returned to you. If possible, keep sight of it.
* Before sending your credit card number over the Internet, make sure you are using a secure connection.
* Tear or shred copies of credit applications or monthly statements before discarding them.
* If a card is lost or stolen, contact the credit card company immediately.

Appendix 7.03F

**Tips for Protecting Yourself against Identity Theft, continued**

If you lose your wallet or it is stolen, or suspect you are a victim of identity theft, *ACT QUICKLY* to minimize damage.

* 1. Call credit card companies to report missing cards. Then follow the call with written confirmation.
  2. File a police report.
  3. Contact your bank if you are missing ATM cards or checks.
  4. Contact the three national credit-reporting agencies to place and ID Theft Alert on your credit file.
  5. Contact the Social Security Administration to report missing Social Security Number or card.
  6. Seek other help and information from agencies such as the Federal Trade Commission and the Identity Theft Resource Center.

### Liability

1. **Credit Cards** – The Truth in Lending Act limits a person’s liability for unauthorized credit card charges to $50.00 per card. To take advantage of this law, a person must write a letter within 60 days of the first bill containing the error. If an individual’s card has been stolen, it should be reported and canceled immediately.
2. **ATM & Debit Cards, Electronic Funds Transfers** – The Electronic Funds Transfer Act provides protection. The amount a person is liable for depends upon how quickly he/she reports the loss. If a person reports a lost or stolen card within two days, they are liable for a maximum of $50.00. Within 60 days, a person is liable for up to $500.00. After 60 days, a person may be liable for all of the money. A person should always telephone the financial institution then follow up in writing to report any losses.
3. **Checks** – Stop payment immediately and ask the financial institution to notify the check verification service. Most states hold the financial institution responsible for losses of a forged check if the person notifies the bank within a reasonable time.