PROTECT YOUR IDENTITY

INFORMATION COMPILED BY
THE ALABAMA DEPARTMENT OF MENTAL HEALTH
OFFICE OF ADVOCACY SERVICES
ORIGINALLY DISTRIBUTED MAY 2008
UPDATED SEPTEMBER 2012

Most honest, hardworking people have given little thought to Identity Theft or its dangers. Some are completely unaware that such a crime exists and others simply believe that it is just something you see on T.V. The task of compiling this booklet was undertaken with three goals in mind. The first goal was to educate consumers about the risks of sharing their personal information and what measures they could take to protect themselves against identity theft. The second goal was to supply service providers with the information they would need to support consumers in their endeavors to protect themselves and should the need arise, to help them respond to being victimized. The third goal was to supply the management of service agencies with this information prompting them to assess their agency's practices with regard to the necessity of having every piece of personal identification information they collect about their consumers, where and how they secure it and who has access to it.

WHAT IS IDENTITY THEFT?

According to the Alabama Attorney General's website:

"Identity theft occurs when your personal identifying information, is stolen by someone. Many identity thieves use stolen information to open fraudulent credit card accounts in your name, to apply for utilities and cell phones in your name, to borrow money in your name, and to make major purchases such as houses and cars in your name. Other identity thieves may even use your identity when arrested or interrogated."

There are some startling facts about Identity Theft:

- Identity Theft is said to be the fastest growing crime in America.
- It can sometimes take years before a person realizes they have been victimized.

- Victims can sometimes spend a great deal of money and time trying to clear up the mess caused by an identity thief.
- The thief is often someone the victim has some type of contact or relationship with such as a work acquaintance, a service or healthcare provider, merchant, friend or even a family member.
- In 2006, Alabama was ranked 27th among the 50 states for the highest number of victims of Identity Theft. There were 2,774 reported victims in Alabama and 246,035 victims nationwide in that study.

Since the data for 2006 shows that identity theft victims in Alabama accounted for only a little over 1% of the total number of victims in the nation, some might believe that too much emphasis is being placed on this problem. However, Identity Theft Victims would probably voice another view. Victims might borrow a quote from Benjamin Franklin, "An ounce of prevention is worth a pound of cure." Victims report spending a great deal of energy, time and sometimes money to straighten out what could have been prevented if they had only known what to do.

HOW CAN I PROTECT MYSELF?

For each of us the first line of defense is good common sense. You may be thinking that you simply do not know where to begin because you have no idea how the thieves access you personal information. Let us examine a few ways your information can be gathered along with common sense precautionary measures you can take.

How an identity thief obtains information……

- Stealing credit cards, ATM cards, social security cards, driver's licenses, passports or checks from purses or wallets.
- Stealing mail, such as credit card applications, bills, or other forms of "junk mail".
- Listening to cell and cordless phone conversations.
- Posing as a telemarketer or representative of a financial institution in order to obtain information.
- Setting up unsecured or bogus web sites.

- "Phishing" also known as sending a fake/cloned website or sending fake emails on the internet.
- Stealing computers and obtaining information from them.
- Digging through trash cans, also known as "dumpster diving".
- Hacking into merchants' databases.
- Removing information from medical/hospital records or other business records.

How to protect against Identity Theft……..

- Check your credit every year; a person is allowed one free credit report every year from each of the three major credit reporting companies. It is recommended to stagger the requests and obtain one report every four months.
- Cross cut (shred) any documents/mail that may contain personal information prior to throwing it into the garbage, this includes unwanted credit card offers. To reduce unwanted mail, contact 1(888) 567-8688.
- Do not carry a Social Security card, passport, or birth certificate in your wallet/purse until the documents are needed.
- Carry only the credit cards/ATM cards you need that day. The use of Debit cards is discouraged due to the amount of loss a victim could suffer to his/her checking account.
- Review credit card and bank statements monthly to ensure there are no charges that you did not make.
- Prepare a list of all credit cards, debit cards, banking accounts and investments. The list should include account numbers, expiration dates, and telephone numbers of the customer service and fraud departments. Place this list in a secure area you can access should your cards be lost or stolen.
- When you have your checks printed include only your name/initials and address or post office box on the check. Do not have your social security number or driver's license number printed on them.
- Sign checks with gel ink, it cannot be easily removed by thieves.
- Pick up new checks at the bank or from a post office box, do not have them mailed to your home. They could be stolen from your mailbox.
- Store your cancelled checks in a safe place.
- Consider placing a lock on your mailbox, or obtaining a Post Office Box. If you are going out of town, have your mail delivery stopped until you return.
- Do not place mail/bills in an unsecured mailbox. Take it to the post office or to a postal service receptacle.
- Never give out information over the telephone from a call that was not initiated by you. If someone does call, and you are concerned there may be a true need for you to provide information, obtain the telephone number from your files or the telephone directory rather than using a number supplied by the caller. Call the

business, explain the call you received and see if information is needed from you. (To reduce unwanted telemarketing calls, register on the National DO Not Call List by calling 1-888-382-1222; TTY is 1-866-290-4236. You must call from the number where you do not wish to receive the calls.)

- Never give out personal information over the internet unless it is on a secured website. The website address should have https:// instead of http://' to indicate it is secured. Also look for the lock icon in the lower right hand side of your screen.
- Do not respond to e-mails that you have not solicited, especially if they are requesting you to provide personal information. Companies you do business with have your personal information and should personalize your e-mail.
- Never use a link provided in an e-mail, instead type the web address into the browser.
- Use a credit card when shopping online as opposed to a debit card. The credit card provides more fraud protection.
- Install a firewall and virus protection on computers to prevent hackers from obtaining information.
- Keep computers locked in a safe area.
- Before disposing of a computer, use a "wipe" utility program to remove data.
- Be careful to whom you give your social security number. If you are asked for this information, ask the person why it is needed, where it will be stored and who will have access to it. Also ask what will happen if you do not supply the number. Ask companies to use a different number than your social security number for identification purposes.
- If it is necessary for you to supply your Social Security number, do not state it loudly in a public place. Instead, write the number down on a piece of paper or whisper the number. If you write the number on a piece of paper, make sure to take the paper with you and destroy it by shredding.
- Store personal information in locked file cabinets or in a safe. If you keep your information at your fingertips such as on a rolodex, rethink your filing system, a thief could take the whole rolodex or a few cards and you might not even notice until you reached for it the next time.

How you may find out you are a victim of identity theft……..

- When bill collection agencies contact a person about overdue debts, they never incurred.
- When a person applies for a loan and learns that their credit history is preventing approval and they thought they had an excellent credit history.

- When something is received in the mail regarding an apartment they never rented, a home or car they never purchased or a job they never worked.
- When monitoring bank accounts and credit reports.

If you have been victimized.....

- Immediately contact the fraud departments of any one of the three consumer reporting companies to place an initial "fraud alert" on your credit report, which will remain for 90 days. A "fraud alert" means that any time a company checks the person's credit for an issuance of a new card on an existing account, to open a new account or to increase limits; extra precautions are taken to ensure that the additional credit is given to the correct person and not the identity thief.

  The three major consumer reporting companies are:
  Equifax 1-800-525-6285, and write P.O. Box 740241, Atlanta , GA 30374-0241;
  Experian 1-888-397-3742, and write P.O. Box 2002, Allen, TX 75013;
  TransUnion 1-800-680-7289, and write Fraud Assistance Division, P.O. Box 6790 Fullerton, CA 92834-6790
- Contact each of your creditors to report any account that has been tampered with or opened fraudulently and close the accounts. Ask them to send their company's "fraud dispute" forms for you to fill out or ask if they will accept the Federal Trade Commission's ID theft affidavit.
- Make a list of all of the financial institutions you do business with (credit card companies, institutions where you have checking, savings, and investment accounts, telephone, cell phone, utilities and internet service providers). Contact the companies and have them place a "fraud alert" on your account.
- File a complaint with the Federal Trade Commission (FTC) and keep a copy of the complaint.
- File a police report with the local police or with the police in the community that the theft has taken place. Provide them with a copy of the Federal Trade Commission ID Theft Complaint Form; make sure to obtain a copy of the police report. If the police say they cannot take a report, be persistent and remind them of the importance of having a police report. If they still refuse, call the sheriff's office and ask to file a report. If denied there, call the Attorney General's Office.

- Submit a copy of the police report to one of the major credit bureaus to have an "extended fraud alert" on the credit file for a 7 year period.
- Continue to review all credit, billing, and bank statements after you have been the victim of identity theft and report all questionable activities to the appropriate company or financial institution immediately.
- Once the identity theft dispute has been resolved with the company, request a letter stating the company has closed the disputed accounts and has discharged the fraudulent debts. This will provide proof in the event errors relating to the theft reappear on the credit report.

If items have been stolen.....

- If ATM or Debit Cards have been stolen, immediately notify the bank or card issuer, even if you are unsure they have been used. If you obtain new accounts from creditors, make sure new Personal Identification Numbers (PINs) and passwords are given.
- If checks have been stolen, alert the bank and close the bank account. Ask the bank to notify check verification companies and alert them about the potential identity theft; ask them to stop accepting checks on the account being closed. The major check verification services are:
  Telecheck (800) 710-9898 0r (800) 927-0188,
  Certegy, Inc. (800) 437-5120,
  ChexSystems (800) 428-9623,
  SCAN (800) 262-7771
- If credit cards or charge cards have been opened in your name, have the accounts closed and use the fraudulent account affidavit to dispute the charges.
- If existing credit card accounts have been tampered with, have new account numbers assigned and make sure they are protected by passwords. If you make purchases on the internet using these cards, you may need to notify the merchant sites where you shop so they will no longer accept your card.
- If a driver's license has been stolen, request a new driver's license from the Department of Motor Vehicles. Also request to have a fraud report attached your driving record.
- If it is suspected that an address had been fraudulently changed, contact the US Postal Service and notify them of the suspicion that an identity thief has filed a change of address with the post office. Also notify the local postmaster that mail in your name should go to your address.
- If a passport has been stolen, contact the United States Department of State at (877) 487-2778;

TTY (888) 874-7793.

- If there are charges on a utility, cell phone or telephone service that were not made by you, the company should be contacted immediately. The account may need to be closed and new accounts opened.
- If your Social Security Card has been stolen, apply for a replacement card with Social Security. Also request Social Security to review earnings to ensure they are correct and no one else has been using the social security number to work. Only as a last resort should you change Social Security numbers, as this may create complications for you later.
- The Internal Revenue Service should be contacted if you suspect your identification has been used in connection with tax violations.
- If you receive a statement regarding medical procedures you did not have, contact the source of the statement (healthcare provider or insurance) immediately to see if there has been some mistake. If you discover you are a victim of medical identity theft, contact the Medical Information Bureau at 1-866-692-6901;TTY 1-866-346-3642 to alert them and to make sure that your report is corrected and your information is accurate.

When contacting companies in regard to the identity theft……

- By law, companies must provide a copy of the application or other business transaction record relating to the identity theft if the request is submitted in writing. Companies should also review the claim and send a written response telling the outcome of their investigation.
- Keep a record of all correspondence and conversations with financial institutions, credit bureaus and law enforcement officials. (See the chart in the back of this booklet)
- Send all correspondence by certified mail, "return receipt requested" and document what the company received and when. Keep <u>copies</u> of everything, do not send originals of supporting documents, send copies!

Until the identity thief is identified and stopped, the theft may be ongoing. You may become frustrated and think it is easier to pay disputed charges; this is not recommended! If you are unable to resolve disputes with creditors and credit bureaus, then the Alabama Attorney General's Consumer Protection Section (1-800-392-5658) may be able to assist by mediating the dispute between you and the creditor. If this does not work then you may need to seek assistance from a lawyer.

If you need help…

- If you have your identity stolen you may find that it causes you to worry and be distressed or even depressed, if so, be sure to talk to someone about it.
- You may seek help from Mental Health Professionals to obtain emotional support and counseling, as well as have any necessary referrals made to Case Management or other resources.
- If you need assistance with filing the reports for the legal, governmental, and financial institutions, ask your Mental Health Professionals for help. If they can not assist you they will refer you to someone who can.

As you can see there is a great deal of information to remember and to retrieve if ever needed. The remainder of this booklet is devoted to the organization of this material. The first chart (page 10) is organized by the types of items which might be used to steal a person's identity. The second chart (page 29) is a listing of agencies (by type) which can provide assistance in the reporting and resolution of an identity theft. The third chart (page 37) is a listing of websites you can visit to read more about identity theft. The fourth chart (page 40) is a worksheet which may be used to document actions taken to resolve an identity theft. The fifth chart (page 42) is to be used for any other calls you may make either in trying to protect your identity or trying to resolve an identity theft.

All information came from the agencies you see listed on the first three charts. Telephone numbers were accurate as of the first distribution of this booklet. Please use discernment when using these resources as we have no firsthand knowledge of the usefulness of their services.

CHART 1. THE ITEMS USED TO STEAL AN IDENTITY, PRECAUTIONS TO TAKE AND RESPONSES TO VICTIMIZATION

Note: Anyone knowingly submitting false information could result in that person being prosecuted for perjury.

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
CARDS, (ATM, Banking or Credit) ***For other cards such as Social Security, Driver's License etc. see "Government Issued Identification" in this chart.***	• Sign the back of your cards. • Only carry what you need. • Safely store the others. • Keep a listing of what you carry so if your wallet is lost or stolen you can immediately cancel cards and get new ones. • If you have to replace your cards, use new PIN also. • Never give your PIN to <u>anyone</u>. • Always shield the machine where you are entering your PIN so that others can not see it.	• Review your statements as soon as they come in the mail. Check for transactions you did not make, if you find any, act immediately! • Pay attention if the statements do not come at the time they should a thief could have arranged to have them sent to another address. • Check your credit report. You are entitled to one	• If you find transactions you did not make on your statements, contact the bank or Credit Card Company immediately. • Notify the Federal Trade Commission and keep a copy of your report. • If your credit cards or banking cards were stolen, immediately contact the fraud departments of any of the three consumer reporting companies to place a "fraud alert" on your credit report. (You will need to provide your Social Security Number to do this.) This means that if the thief tries to access your credit such as getting a new account, new card or increasing the limits, then special precautions are taken to make sure he/she is not successful. This alert will remain on your credit file for 90 days. • Notify the local police and/or the police in the community the theft occurred. They may suggest you file a report on line but try to do so face to face even if you must go to the station. Get a copy of the

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	• Memorize your PINs, do not write them down and carry them with you. • When deciding on a PIN do not use dates important in your life, any part of your social security number or the numeric equivalent of your mother's maiden name or a pet's name. These are easily discovered by a thief. • DO NOT CARRY YOUR SOCIAL SECURITY CARD IN YOUR WALLET OR PURSE! (See Social Security in this listing for more information.)	free report from each of the 3 credit reporting bureaus each year. You could manage to get a free report every four months. • Always check on any unexplained denial of credit.	report. If they tell you they can not do a report be persistent, remind them of the importance of having a police report. Provide them with a copy of the Identity Theft form you submitted to the FTC. If they will not file a report go to the Sheriff's Office, if that office will not file a report, go to the State Police and if they will not file a report, call the Attorney General's Office (1-800-626-7676). • If your debit or ATM card is stolen, contact the company immediately, and follow up in writing. The account may have to be closed and a new one opened. Request a new card with a different number and password. (The amount of stolen money you are liable for is based on how quickly you alert the bank. If you report within 2 days your losses are limited to $50.00 wait any longer and you may have to pay a great deal more.) Different institutions regulate different types of banks. If you are having a problem with your bank, ask which institution regulates it or visit www.ffiec.gov/enforcement.htm to determine which institution you should contact. • Follow up any verbal reporting with a written report. If you are sending any documents, do not send originals, send copies instead. (The exception to this rule is any form the company asks you to fill in and submit to them. You may send the original but keep a copy.) Some companies may accept the FTC ID Theft Affidavit, you will have to ask. Also ask for the proper mailing address. For FTC Affidavit form see:

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
			www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf • Always send items by registered mail "receipt requested" to the address the company has provided for their business so you can prove what was sent and when they received it. • Submit a copy of the police report to one of the major credit bureaus to have an extended "fraud alert" on the credit file for a 7 year period. • Continue to review all credit, billing and bank statements after you have been the victim of ID theft. Report all questionable activities to the appropriate company or financial institution as soon as possible. • Once the ID theft has been resolved with the company, request a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This will provide proof in the event errors relating to the theft reappear on the credit report. • Keep copies of all correspondence. Always keep the originals of correspondence sent to you. • Keep this file permanently. • If you need help clearing up fraudulent charges from your credit report you can contact Consumer Credit Counseling Service (CCCS) 1-800-251-2227. • If you have established accounts with businesses online using the credit card which was lost or stolen, you will want to change your passwords with those retailers.

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
CHECKS	• Do not put your driver's license or Social Security # on your checks. • Do not have new checks delivered to your home. Have them delivered to the bank and go by and pick them up there. • Do not leave new or canceled checks laying around so that they are easily picked up by people coming into your home. Store them in a safe place. • Carry only the number of checks you will need to conduct your business. • Always write checks in non-erasable ink.	• Review your bank statement as soon as you get it. • If a merchant refuses your check, find out why. Ask for the contact information for their check verification company. • If you get a call from someone saying your check has bounced and you know you have sufficient funds to cover the check, hang up and call your bank immediately to find out what has happened.	• If your checks have been stolen, stop payments on the missing checks and close the bank account. • If one of your checks is forged you should contact Chex Systems, Inc.: 1-800-428-9623; www.chexhelp.com; Fax: 602-659-2197. Address: Chex Systems, Inc. Attn: Consumer Relations; 7805 Hudson Road, Suite 100; Woodbury, MN 55125. • Notify the major check verification companies so that they can let retailers know not to accept your lost or stolen checks. TeleCheck at 1-800-710-9898 or 1-800-927-0188 and Certegy, Inc. at 1-800-437-5120. • If your checks have not been lost or stolen and you find activity in your account(s) which you did not initiate, contact the bank to report it, close the account and open another. Establish new passwords and/or PINs. Remember not to use dates or names which are important to you because they might be easily guessed. • Check to find out if bad checks have been passed in your name, call: SCAN 1-800-262-7771. • Contact Chex Systems, Inc. to review your consumer report to make sure that no other bank accounts have been opened in your name. 1-800-428-9623; www.chexhelp.com; Fax: 602-659-2197. Address: Chex Systems, Inc. Attn: Consumer Relations; 7805 Hudson Road, Suite 100; Woodbury, MN 55125.

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
			• Dispute any bad checks passed in your name with merchants so they don't start collection actions against you. Find out if they have a special form they wish for you to use otherwise use the forms in the back of this book to pattern your letter after. • If you have trouble getting your bank to help you resolve your bank-related identity theft, contact the agency that oversees your bank. Call the bank and ask them for the name of the agency or go to the National Information Center of the Federal Reserve System at www.ffiec.gov/nic/ then click on "Institution Search." • If you pay bills through automatic deduction from an account you have closed, make sure you notify the businesses with the new arrangements for them to receive payment so your services, whatever they may be, will not be interrupted.
COMPUTERS ***(E-mails and Internet Usage)***	• Make sure your personal computer is equipped with up-to-date security and virus protection software so that no one can tap into your information without your knowledge. • Always log off of your computer when it is not in	• Your computer reacts slowly. • You start getting junk emails when you have not been getting them. • The computer does not	If you believe you have been victimized by any means involving the use of the Internet, you should file a complaint with the Internet Crime Complaint Center at www.IC3.gov .

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	use. • Do not leave your passwords laying around where they may be found. • Do not allow the computer to save your passwords so you do not have to log in. • Do not use passwords that are easy to guess such as your pet's name or your birth date. • In your password use both upper and lower case characters and both symbols and letters. • Do not download files, launch attachments, or click on hyperlinks from people you do not know. You could be exposing your system to a virus. • Use a firewall program to help prevent unauthorized people from accessing your computer. • Always use a secure browser to protect the security of your online	respond to some commands. • Make sure you check your credit report at least annually.	

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	transactions. • Before disposing of a computer, remove data by using a strong "wipe" utility program. Do not rely on the "delete" function to remove files containing personal information. • Never provide personal information when requested by an e-mail. • If for instance, you receive an email from your bank, do not supply the information they request but rather call your bank using a telephone number you find in the yellow pages or on a bank statement. Do not call a number listed on the email. • Do not respond to e-mails saying you have inherited money or which offer money for helping them transfer money to an account. This is a scam! Delete the e-mail. Always		

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	remember if an offer sounds too good to be true, it probably is. • Never send money anywhere to anyone to collect a prize. It is a scam! • Never allow someone you met on the internet (or anywhere else) to send a package to you for you to send on to someone else. This is a scam and you may be sending illegal or stolen goods and can be prosecuted. • Be very careful about giving out information over the Internet. • If you choose to shop using the Internet make sure the website you are using is secure before you enter your information. Check the web address in your browser's address bar to see if it says https:// instead of http://. Also make sure there is an icon		

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	of a lock at the bottom of the web browser page. • Never use your debit card to purchase items on line. • Use a credit card or charge card so that you have the protection of the Fair Credit Billing Act. • Never use a link provided in an email to go to a shopping site. (It could be a fake site.)		
DOCUMENTS	• Shred anything containing personal information before you throw it away. • Store documents containing personal information properly. Do not leave things laying out so that they can easily be picked up by anyone coming into your home. • Keep business files neatly stored. If someone should tamper with your documents, you will notice more so than if you do not store them in an organized manner.	Check your Credit report.	

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	• Store deeds, mortgages, income tax records and stocks and bonds in a secure place.		
EDUCATION	A thief may call claiming to be able to get your child a scholarship for a very small "processing fee" if you will give your credit card number. This is a scam! • Do not give any information over the telephone. Instruct children not to give their information. • When looking for scholarship money, go to reputable sources such as the free information on www.FederalStudentAid.ed.gov.	There have been instances where individuals find student loans have been taken out in their names. They discover this when they get their credit report or the loan comes due.	• If you receive one of these calls or another contact which makes you suspicious contact the Office of Inspector General's hotline at 1-800-MIS-USED (1-800-647-8733) immediately. Send an email to oig.hotline@ed.gov FAX: 202-245-7047 or Write: US Department of Education Inspector General; 400 Maryland SW; Washington, DC 20202-1510 • Contact the Federal Trade Commission at 1-877-FTC-HELP (1-877-382-4357 or www.ftc.gov/scholarshipscams
GARBAGE	• Shred all pre-approved credit card applications, catalog order blanks, discarded banking information, expired credit cards, ATM or credit card receipts, insurance or health information or anything else that has	You may not detect that someone has stolen the items you consider garbage until something happens such as you receive a call from a bill collector about an account	The action to be taken depends on the damage that was done. See the FTC's recommended general response to ID Theft in the front of this manual.

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	personal information on it before discarding them. Identity thieves do not mind getting dirty to get your personal information from these documents. • Reduce the amount of junk mail you get. Dial 1-888-5-OPT-OUT (1-888-567-8688) to be removed from the database that generates credit card pre-approval offers.	you know nothing about or you are denied a loan even though you have always paid your bills on time.	
GOVERNMENT ISSUED ID ***(such as Driver's License, Social Security Card or Passport.)***	• Do not leave such identification unsecured so others have access to it. Once someone has your Social Security Number all kinds of business can be conducted under your name. • Make sure you know where your wallet is at all times. You may think you are safe and among friends. Remember, most victims are acquainted in some way with the thief. If possible lock up your purse	You may not know someone has used your information for years after you discover the items missing. • You may begin to get calls or letters about bills you know nothing about. • You may get a statement from Social Security about your work history and see	• If your Social Security Card is stolen or you have reason to believe someone is using your Social Security Number, Contact the Social Security Administration and ask for an Earnings and Benefits Statement. 1-800-772-1213 or www.ssa.gov or the Fraud Line at 1-800-269-0271. • If your Driver's license is stolen, request a new one from the Department of Motor Vehicles in your area by going to the office in person. Also request to have a fraud report attached to your driving record. • If your Passport is stolen, contact the U.S. Department of State at 1-877-487-2778. • React quickly if you believe you are a victim. The faster you act, the more likely you are to put a stop to this criminal's activities with regard to you. Also the more likely he/she will be caught and

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	or wallet when you are involved in an activity which prohibits you from carrying it on your person. • Never give your social security card or driver's license number to anyone on the telephone. • Question why the numbers are needed if someone asks you for them. • Never give your Social Security number verbally if others are present, instead, write it down and let the person see it. Then shred the paper.	activity that you know is not yours. • You may be contacted about a crime committed in your name. • You may get credit cards or statements from accounts you did not open. • You may be denied credit when you try to open an account. • You may get statements regarding medical procedures that you did not have done. • Always check your credit report.	prosecuted. • Even though it could be a matter of a simple error being made, do not assume that is the case. Always follow up on anything which does not seem quite as it should be. • Always request an explanation for any denied credit, refusal to approve checks etc.
MAIL	• Drop bill payments in a	You should suspect	• Report mail tampering to the Postal Inspection

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	Postal Service box rather than place them in your home mailbox for pick up. • Collect your mail from your home box daily. • If you are going to be out of town have the Post Office hold your mail until you return. See: https://holdmail.usps.com/duns/HoldMail.jsp . Then have it delivered to your home or pick it up at the Post Office. • Consider installing a locking mailbox or getting a P.O. Box. • Reduce the amount of junk mail you get. Dial 1-888-5-OPT-OUT (1-888-567-8688) to be removed from the database that generates credit card pre-approval offers.	someone may be tampering with your mail if: • Your bills do not arrive on time. • Your volume of mail decreases. (Someone could have changed your address.)	Service at 1-877-876-2455. • If you suspect a fraudulent change of address has been submitted to the US Postal Service contact them at 1-800-ASK-USPS (1-800-275-8777) and let them know. Also notify the local postmaster and make sure your proper address is noted. There are forms on the website http://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx
MEDICAL	• Do not give information such as your insurance	• Review any statements	If you discover that someone has received medical services under your information, you should immediately

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	(including Medicaid and/or Medicare) numbers to just anyone. • Ask your medical service provider how your information is secured.	about the medical services you have received and question any mistakes.	notify your insurance provider and the Medical Information Bureau. 1-866-692-6901 (TTY: 1-866-346-3642).
PINs/ PASSWORDS	• Never use your Social Security Number or anyone else's as a PIN or password. Do not even use the last four digits. • Never use your mother's maiden name, your birth date; your middle name, your pet's name or anything that could be easily discovered by thieves. • Create passwords that combine 6-8 numbers, symbols and letters, upper and lower case. • You might think of a favorite line of poetry, a phrase or a song (but not one you mention often so others can guess what it is) and choose the first or last	• You may discover charges or withdrawals you did not make.	If your PIN or Password has been compromised, cancel that PIN or Password immediately. Contact the bank or merchant for assistance in obtaining a new one. In some cases you may have to establish a new account.

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	letter of each word and include numbers where they would look like or count the letters such as: Row, row, row your boat, gently down the stream might become the password R#3ybgdts!		
RECORDS, ***(Business, Healthcare, Service, and Work Records)***	• Ask these agencies what precautions they take to safeguard your information. • Do not give your personal information to just anyone in the agency but only to those who have a need to know. • If asked for your Social Security #, ask why it is needed and how it will be protected. See if some other identifier can be used. (Keep in mind there are some financial/ insurance/business transactions which do require your SS #.) • Never give your Social Security number verbally if	• Check statements received from insurance and healthcare agencies to see that the services rendered match the healthcare you have received. If not, someone may be getting healthcare using your information. Aside from causing financial problems, it could place you in danger in the event you become ill. Caregivers may	• Social Security Administration Fraud Line 1-800-269-0271 if you believe someone is using your Social Security Number. If you discover that someone has received medical services under your information, you should immediately notify your insurance provider and the Medical Information Bureau. 1-866-692-6901 (TTY: 1-866-346-3642). • Contact the IRS if you believe someone has committed tax fraud using your identity. www.irs.gov

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	others are present, rather write it down and let the person asking for it see it then shred the paper.	use the thief's information upon which to base their treatment instead of yours. • Always review all financial records for accuracy. • Check the annual Social Security Statement of employment for accuracy. If you see additional work you did not do, someone may be working under your ID and not paying taxes. This could cause you major problems with the IRS.	
SOCIAL SECURITY CARD	• <u>DO NOT CARRY YOUR SOCIAL SECURITY CARD IN YOUR WALLET!</u>	• If your Social Security Card has been lost or	• Contact the Social Security Administration Fraud line at 1-800-269-0271 or at P.O. Box 17768, Baltimore, MD 21235. • Do not get a new Social Security number issued unless it is

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	• Store it in a safe place. • Only take it with you on days you may need it such as when you start a new job. • Memorize your Social Security number. • If asked for your Social Security #, ask why it is needed and how it will be protected. See if some other identifier can be used. (Keep in mind there are some financial/insurance/ business transactions which do require your SS #.) • Never give your Social Security number verbally if others are present, rather write it down and let the person asking for it see it. Then shred the paper. • Protect your children's social security numbers. Request credit reports for your children to insure no one has used their numbers to set up debts they would	stolen, contact the Social Security Administration at 1-800-772-1213. • Ask for a statement of your earnings to see if someone has been working using your Social Security number. • Check the Social Security numbers of your children who are not yet legal age.	absolutely necessary because it could cause you additional problems. • If you suspect there have been tax violations using your social security number or other information, you should contact the Internal Revenue Service at 1-800-908-4490.

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	not know about until adulthood when they try to establish a line of credit. • Teach your children to guard their Social Security Numbers.		
TELEPHONE, Cell and Landline	• If at all possible do not conduct business which requires giving personal information using a cell phone. Landlines are more secure. • Do not make business calls when others are around and might overhear. • Do not give anyone who calls your home your personal information. If the caller says he is from your bank and needs the information from you, hang up and call the bank using the number in the yellow pages or from a bank statement not the number you are given by the caller. Use the same technique for supporting	Check your bill when it arrives to make sure you are responsible for all the charges.	If there are charges you know nothing about, contact your telephone company immediately.

TYPE OF ITEM	PRECAUTIONS	HOW TO FIND OUT IF YOU ARE A VICTIM	RESPONSE TO VICTIMIZATION
	charities. • Thieves may try to sell you vacations at low rates, promise prizes and/or other enticements to get you to give them your personal information or credit card number. Don't! • Reduce the number of telemarketing calls you receive by registering your telephone number with the National Do Not Call List by calling 1-888-382-1222. You must call from the telephone to which you want the calls to stop coming.		
UTILITIES	• Review your utility bills carefully.	• Make sure to question any charges that do not appear to be yours.	• If there are charges on your electric, gas, telephone or cell phone bills which you did not make, contact the utility company immediately. The accounts may need to be closed and new ones opened. • If utilities, telephone service, and/or cell phone accounts have been opened in your name, notify the companies in writing that you dispute the accounts. • Contact the Federal Trade Commission for fraud involving long distance providers and cellular phones.

CHART 2. RESOURCE LISTING

Note: Anyone knowingly submitting false information could result in that person being prosecuted for perjury.

AGENCY	FUNCTION	CONTACT INFORMATION
ALABAMA ATTORNEY GENERAL'S OFFICE	Consumer Protection Hotline	1-800-392-5658 or www.ago.alabama.gov www.familyprotection.alabama.gov/identity.cfm?Action=3
BANK REGULATING INSTITUTIONS **(Remember to find out which one regulates your bank.)** For assistance if a bank is not assisting you to clear up a bank-related identity theft problem.		
Federal Deposit Insurance Corporation	Supervises state-chartered banks that are not members of the Federal Reserve System, and insures deposits at banks and savings and loans.	1-877-275-3342; or www.fdic.gov/consumers or write: FDIC Division of Compliance and Consumer Affairs 550 17th Street, NW Washington, DC 20429
Federal Reserve System	Supervises state-chartered banks that are members of the Federal Reserve System.	www.federalreserve.gov or write: Federal Reserve Board Consumer Help P.O. Box 1200 Minneapolis, MN 55480. 1-888-851-1920; TTY 1-877-766-8533; or contact the Federal Reserve Bank in your area. There is one in Atlanta.
National Credit Union Administration	Charters and supervises federal	Call: 1-800-827-9650; 1-800-755-1030;1-800-778-

AGENCY	FUNCTION	CONTACT INFORMATION
Office of Examination and Insurance	credit unions and insures deposits at federal credit unions and many state credit unions.	4806. or write: Compliance Officer National Credit Union Administration 1775 Duke Street Alexandria, VA 22314
Office of the Comptroller of the Currency (OCC)	Charters and supervises national banks. If the word "national" appears in the name of a bank, or the intials "N.A." follow its name, the OCC oversees its operation.	1-800-613-6743; TDD 713-658-0340 FAX: 713-336-4301 or write: Customer Assistance Group 1301 McKinney Street Suite 3710 Houston, TX 77010
Office of Thrift Supervision (OTS)	The primary regulator of all federal, and many state-chartered, thrift institutions, including savings banks and savings and loan institutions	1-800-842-6929; TTY 1-800-877-8339 Office of Thrift Supervision 1700 G Street, NW Washington, DC 20552 Email: consumer.complaint@ots.treas.gov
BETTER BUSINESS BUREAU	You may check to see if this bureau has received complaints about the business you are about to do use. You may also file a complaint about the practices. This site has a number of tips on avoiding identity theft.	www.bbbonline.org/idtheft/protect.asp 1-703-276-0100 Council of Better Business Bureaus 4200 Wilson Blvd. Suite 800 Arlington, VA 22203-1838
CHECKS		
Check Verification Services:	These are the agencies merchants check with before accepting a check in payment for goods or services.	
Certegy Inc.	You may report lost or stolen checks to this agency.	1-800-437-5120; Fax: 727-570-4936 www.certegy.com or write:

AGENCY	FUNCTION	CONTACT INFORMATION
		Certegy Check Services, Inc. P.O. Box 30046 Tampa, FL 33630
TeleCheck	You may report lost or stolen checks to this agency.	1-800-710-9898 Fax 713-332-9300 or 1-800-927-0188 for lost or stolen checks or write: TeleCheck Consumer Affairs P.O. Box 4451 Houston, Texas 77210-4451 or www.telecheck.com
Chex Systems, Inc.	Produces consumer reports about checking accounts (just as credit bureaus do about consumer credit) and is subject to the Fair Credit Reporting Act. You can request a free report each year. You may opt-out of having your address shared with marketers with Chex Systems, Inc. at 1-877-OPTOUT 5 (1-877-678-6885).	1-800-428-9623; or www.chexhelp.com Fax:602-659-2197 or write: Chex Systems, Inc. Attn: Consumer Relations 7805 Hudson Road, Suite 100 Woodbury, MN 55125
Shared Check Authorization Network (SCAN), Electronic Transaction Corp.	If you have been denied an account from a bank or credit union, and ChexSystems℠ was used in the decision process, you can order your consumer report to help you understand what led to this decision.	1-800-262-7771; Fax: 1-800-358-4506 SCAN, Electronic Transaction Corp. 7805 Hudson Road, Suite 100 Woodbury, MN 55125 www.scanassist.com
CREDIT BUREAUS:		

AGENCY	FUNCTION	CONTACT INFORMATION
Note: The Federal Trade Commission recommends that you go to www.annualcreditreport.com for free annual reports or call 1-877-322-8228 or download the request form at the site listed and mail to: Annual Credit Report Request Service; P.O. Box 105281; Atlanta, GA 30348-5281.		
Equifax	To alert them about your possible identity theft. A call to one alerts all three. You may also order (for a fee) an additional credit report.	1-800-525-6285 or www.equifax.com or www.fraudalert.equifax.com write: Equifax P.O. Box 740241 Atlanta, GA 30374-0241
Experian	To alert them about your possible identity theft. A call to one alerts all three. You may also order (for a fee) an additional credit report.	1-888-397-3742; or www.experian.com or write: Experian P.O. Box 2002 Allen, TX 75013
TransUnion	To alert them about your possible identity theft. A call to one alerts all three. You may also order (for a fee) an additional credit report.	1-800-680-7289; or www.transunion.com or write: TransUnion Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790
Credit Report – Annual – Free	Get your free report annually from each of the three credit bureaus. Order all three reports at one time if you are in the market for credit or have discovered you are a victim. If you have placed an alert on your report ask about your eligibility for additional free reports.	www.annualcreditreport.com or call 1-877-322-8228 or download the request form at the site listed and mail to: Annual Credit Report Request Service; P.O. Box 105281; Atlanta, GA 30348-5281.

AGENCY	FUNCTION	CONTACT INFORMATION
CREDIT CARD COMPANIES		
American Express	Report lost card, check activity etc.	1-800-528-4800 or 1-800-297-7672 or www.americanexpress.com
Discover	Report lost card, check activity etc.	1-800-DISCOVER or 1-800-347-2683; TDD 1-800-347-7449 http://www.discovercard.com/contact-us/
MasterCard	Report lost card, check activity etc.	1-800-627-8372 or www.mastercard.com
Visa	Report lost card, check activity etc.	1-800-VISA911 or 1-800-847-2911 or www.usa.visa.com/personal
CREDIT CARD PRE-APPROVAL OPT-OUT	To stop getting pre-approved credit card applications in the mail.	1-888-5 OPTOUT or 1-888-567-8688
CREDABILITY	Get help clearing fraudulent charges from your credit report.	www.cccsatt.org
DO NOT CALL	To reduce the number of telemarketer calls received. Telemarketers should not call your number once you have been on the registry for 31 days. If they do you can file a complaint at this website.	1-888-382-1222 or www.donotcall.gov TTY 866-290-4236
EDUCATION		
United States Department of Education Office of Inspector General	To report fraud involving grants and loans intended for educational purposes.	Atlanta, GA 1-404-562-6460.
FBI	If someone has committed a crime using your identity, write to the FBI and ask for your criminal history. Include your fingerprints and a check for $18.00. Explain that you are a victim of identity	Criminal Justice Information Services Division 1000 Custer Hollow Road Clarksburg, West Virginia 26306 www.fbi.gov

AGENCY	FUNCTION	CONTACT INFORMATION
	theft. (Make sure to check the website for instructions.) Go to www.fbi.gov , select "Contact Us" scroll down to "Other FBI Websites with Specific Contact Information", and select "Identification Record Request".	
FEDERAL TRADE COMMISSION	To get information about or to report Identity Theft.	About a Company, an organization or a business practice: 1-877-FTC-HELP. About ID Theft: 1-877-IDTHEFT (1-877-438-4338); TTY: 1-866-653-4261 or www.ftc.gov/idtheft write: Identity Theft Clearinghouse Federal trade Commission 600 Pennsylvania Avenue, N.W. Washington, DC 20580
IDENTITY THEFT RESOURCE CENTER	Provides support and assistance to victims of identity theft.	Identity Theft Resource Center P.O. Box 26833 San Diego, CA 92196 or 858-693-7935 or 1-888-400-5530 No Cost Victim Assistance. www.idtheftcenter.org or e-mail: irtc@idtheftcenter.org
INTERNAL REVENUE SERVICE	For people who think they are a victim of identity theft involving their taxes.	Internal Revenue Service P.O. Box 9039 Andover, MA 01810-0939 Fraud Line: 1-800-829-0433 Tax Payer Advocates Office: 1-877-777-4778; Fax 1-978-247-9965 or www.treas.gov/irs/ci
INTERNET		
The Internet Crime Complaint Center	A partnership between the FBI, the National White Collar Crime Center	www.IC3.gov

AGENCY	FUNCTION	CONTACT INFORMATION
	(NW3C), and the Bureau of Justice Assistance (BJA). The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations.	
Stay Safe Online	Provides free and non-technical cyber security and safety resources to the public, so consumers, small businesses and educators have the know how to avoid cyber crime.	www.staysafeonline.info/
LAWYERS		
Alabama State Bar	Can provide names of lawyers who specialize in consumer law and more specifically identity theft. Ask about expertise in the Fair Credit Reporting Act and the Fair Credit Billing Act.	Lawyer Referral Service 415 Dexter Avenue Montgomery, AL 36104 1-800-392-5660 or 334-269-1515 Fax: 334-261-6310 www.alabar.org
Legal Services Alabama	Provides a guide to free and low-cost civil legal services in Alabama and other resources.	1-866-456-4995 or www.alabamalegalhelp.org
OPT-OUT	To reduce the number of unsolicited pre-approved credit card applications received in the mail.	1-888-5-opt-out or 1-888-567-8688
POLICE DEPARTMENTS/SHERIFF'S	Listing of Law Enforcement Office in Alabama	www.usacops.com/al

AGENCY	FUNCTION	CONTACT INFORMATION
OFFICES		
POSTAL SERVICES		
Postal Inspector, USA	If you suspect that an identity thief has used the mail to commit fraud with your identity.	*1-877-876-2455 or* 1-800-372-8347 or 404-608-4500 or Atlanta Division PO Box 16489 Atlanta GA 30321-0489 www.usps.gov/postalinspectors U.S. Postal Inspection Service *475 L'Enfant Plaza* Washington, DC 20260 1-202-268-2284
Postal Service, USA	To have your mail held or to report problems with your mail.	1-800-275-8777 or www.usps.com
SOCIAL SECURITY ADMINISTRATION	To order Earnings and Benefits Statement To report Social Security Fraud	1-800-772-1213 or www.ssa.gov Fraud Hotline: 1-800-269-0271 TTY: 1-800-325-0778

CHART 3. RESOURCES FOR ADDITIONAL READING ON THE TOPIC OF IDENTITY THEFT

Note: Anyone knowingly submitting false information could result in that person being prosecuted for perjury.

AGENCY	FUNCTION	CONTACT INFORMATION
Anti-Phishing Working Group	Site committed to wiping out Internet scams and fraud.	www.antiphishing.org
Direct Marketing Association Mail Preference Service	Will remove your name from or can add your name to individual marketing lists. There are fees for some services.	www.dmaconsumers.org/offmailinglist.html
Call For Action, Inc. (CFA)	Provides information on identity theft resources and complaint forms.	www.callforaction.org
Foundation for Taxpayer and Consumer Rights	Organization to support consumer rights.	www.consumerwatchdog.org
Identity Theft Resource Center	Provides information on children's identity theft.	www.idtheftcenter.org
Junkbusters Corp.	Provides information on how to stop all kinds of junk mail.	www.junkbusters.com
Looks Too Good To Be True	Highlights some of the cons that are on the Internet. "If it looks too good to be true, it probably is."	www.lookstoogoodtobetrue.com
USASearch.gov	A website that gives you a number of resources on the web on identity theft. This site has information on how to recover from identity theft when your social security	www.usasearch.gov Type in "Identity Theft" and you will be given links to government sites with identity theft information.

	number, tax records or mail is involved.	
AGENCY	**FUNCTION**	**CONTACT INFORMATION**
National Association of Consumer Advocates	The National Association of Consumer Advocates (NACA) is a nationwide organization of more than 1000 attorneys who represent consumers victimized by fraudulent, abusive and predatory business practices.	National Association of Consumer Advocates 1730 Rhode Island NW, Suite 805 Washington, DC 20036 (202)452-1989 Fax: 202-452-1989 www.naca.net E-mail: info@naca.net
National Consumer Law Center, Inc.	Provides case assistance and legal research. Provides representation for low income and community based organizations.	National Consumer Law Center, Inc. 77 Summer St., 10th Floor Boston, MA 02110-1006 617-542-8010 or www.consumerlaw.org ; E-mail: consumerlaw@nclc.org
National Center for Victims of Crime	Refers victims of crime to local services.	1-800-FYI-CALL (1-800-394-2255) www.ncvc.org
National Check Fraud Center	Provides information on prevention of fraud and the law.	www.ckfraud.org
National Consumer's League Fraud Center and Internet Fraud Watch	Organization which fights the growing menace of telemarketing fraud by improving prevention and enforcement.	www.fraud.org
National Crime Prevention Council	Includes information for various age groups on protecting themselves against identity theft.	www.ncpc.org
National Criminal Justice Reference Service	Features resources on prevention and resolution of identity theft and other crimes.	http://www.ncjrs.gov
National Organization for Victim Assistance	Organization committed to the recognition and implementation of crime victims rights and services.	www.trynova.org

AGENCY	**FUNCTION**	**CONTACT INFORMATION**
On Guard Online	Provides tips from government agencies and the technology industry to help guard against Internet fraud including how to spot malware on your computer.	www.onguardonline.gov
Privacy Rights Clearinghouse	Provides consumer information and consumer advocacy.	www.privacyrights.org
Private Citizen	Organization which claims to be able to stop junk mail and telemarketers. There are fees for this organization's services.	www.privatecitizen.com
Telemarketing Fraud Educators Toolbox	Provides information on scams and advice to victims.	www.fraud.org/toolbox
University of Oklahoma	Site contains information on prevention, action and resources in one place.	www.ou.edu
US Department of Justice	Provides information about the growing problem of identity theft and where to turn for help.	www.usdoj.gov

CHART 4. DOCUMENTATION OF ACTIONS TO TAKE IF YOUR IDENTITY IS STOLEN

1. **IMMEDIATELY CALL YOUR BANKS, CREDIT CARD COMPANIES, CREDITORS**

BANK/CREDITOR	DATE CALLED	PERSON TO WHOM YOU SPOKE	ADDRESS/PHONE (BE SURE TO ASK FOR THE PERSON'S EXTENSION)

2. **REPORT TO THE CREDIT BUREAUS**

BANK/CREDITOR	DATE CALLED	PERSON TO WHOM YOU SPOKE (BE SURE TO ASK FOR THE PERSON'S EXTENSION)	FRAUD ALERT REQUESTED	NOTES
EXPERIAN **(888)397-3742**				
TRANSUNION **(800)680-7289**				
EQUIFAX				

BANK/CREDITOR	DATE CALLED	PERSON TO WHOM YOU SPOKE (BE SURE TO ASK FOR THE PERSON'S EXTENSION)	FRAUD ALERT REQUESTED	NOTES
(800)525-6285				

3. REPORT TO LAW ENFORCEMENT (USE THE LOCAL PHONE NUMBER FOR YOUR POLICE OR SHERIFF.)

LAW ENFORCEMENT AGENCY	DATE CALLED	PERSON TO WHOM YOU SPOKE (BE SURE TO ASK FOR THE PERSON'S EXTENSION)	REPORT FILED?	REPORT #

4. REPORT TO FEDERAL TRADE COMMISSION AT (877)-ID-THEFT (THAT IS 1-877-438-4338)

DATE CALLED	PERSON TO WHOM YOU SPOKE (BE SURE TO ASK FOR THE PERSON'S EXTENSION)	REPORT #	NOTES

AGENCY CONTACTED	TELEPHONE NUMBER INCLUDING EXTENSION/EMAIL ADDRESS	PERSON TO WHOM YOU SPOKE/WROTE	TOPIC/EXPECTATIONS

CHART 5. DOCUMENTATION OF CONTACTS MADE WHILE PROTECTING IDENTITY OR RESOLVING IDENTITY THEFT