

# Identify Theft White Paper

## What is identity theft?

Identity theft is the term for the criminal act of stealing your personal information to clone your identity with the intent to use it without your knowledge or permission to commit fraud or other crimes.

## How do thieves steal identities?

The following is a list that includes, but is not limited to, the common methods thieves use to steal identities:

1. *Dumpster Diving*: Rummaging through trash to find your personal information.
2. *Skimming*: Stealing debit/credit card numbers and personal information by using special storage devices when processing your debit/credit and ID cards.
3. *Phishing*: Pretending to be financial institutions or companies and sending spam or pop-up messages to get you to reveal your personal information.
4. *Address Change*: Diverting your billing statements to another location by completing a change of address form.
5. *Old Fashioned Stealing*: Stealing wallets and purses, mail including bank and credit card statements, pre-approved credit offers, new checks, or tax information. Stealing personnel records or bribing employees who have access to personnel records.
6. *Pretext*: Using false pretenses to obtain your personal information from financial institutions.

## What do thieves do with stolen identities?

Thieves use stolen identities to:

1. Open new credit card accounts.
2. Change your billing address, run excessive charges on your accounts, pay the minimum amounts due, and drain your accounts.
3. Open new phone or wireless accounts.
4. Set up utility services.
5. Open new bank accounts and write bad checks.
6. Clone your ATM or debit cards to make electronic withdrawals.
7. Take loans.
8. Get driver's licenses.
9. Get government benefits.
10. File fraudulent tax returns.
11. Get jobs.
12. Rent houses or apartments.

## **Identify Theft White Paper**

13. Receive medical services.
14. Give your personal information to police during an arrest.
15. Have dual identities to hide their real identity from the Homeland Security Department.

### **What are the signs of identity theft?**

The following is a list that includes, but is not limited to, signs or evidence to look for to find out if your identity has been compromised:

1. Evidence of bank or credit card accounts being opened in your name without your knowledge or approval.
2. Evidence of charges deducted from your accounts that you did not initiate.
3. Evidence of inaccurate information (e.g. wrong personal information, SSN, address, name, initials, or employers, etc) on your credit reports.
4. Not receiving your credit card bills, bank statements, or other personal mail for no apparent reasons.
5. Receiving credit cards that you did not apply for.
6. Receiving calls or letters from collection agencies or businesses asking you to pay the cost of goods or services that you did not buy.
7. Denying you credit or offering you less favorable terms for no apparent reason, e.g. high interest rate.

### **Deter identity theft by safeguarding your information**

Awareness is an effective weapon against many forms of identity theft. The following is a list, which includes but is not limited to, helpful tips that will help you protect your identity from being stolen:

1. Monitor the activity on your accounts and bank statements on a daily or regular basis.
2. Make sure to receive your bank statements and credit card bills.
3. Check your credit report regularly.
4. Shred any financial documents and paperwork containing your personal information before you discard them.
5. Do not carry your social security card in your wallet. Keep your social security card locked in a safe place.

## **Identify Theft White Paper**

6. Do not write your social security number on checks or similar documents.
7. Do not carry multiple credit cards in your wallet.
8. Do not give out personal information on the phone, through the mail, or over the internet unless you have initiated the contact, and you know who you are dealing with.
9. Be aware that federal and state agencies, credit card companies, and banks only use regular mail and certified agencies to contact you, e.g. USPS, UPS, FedEx, etc.
10. Never click on links sent in unsolicited emails.
11. Never open any emails you receive from unknown sources.
12. Use firewalls, anti-spyware, and anti-virus software to protect your personal computer; keep these tools up-to-date at all times.
13. Do not use an obvious password like your birth date, your mother's maiden name, your pet's name, or the last 4 digits of your SSN.
14. Use a strong password combination that includes numbers combined with both upper and lower case characters. Do not make your password too complicated so you cannot remember it.
15. Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, have work done in your home, or have social gatherings.

### **What should you do if your identity is stolen?**

The following is a list, which includes but is not limited to, tips that help you know what to do if you become a victim of identity theft:

1. File a police report.
2. Inform the three credit bureaus so they can monitor your accounts
3. Put a fraud alert on your accounts.
4. Seek immediate legal advice.
5. File a report with the Federal Trade Commission (FTC).
6. Notify your creditors.
7. Dispute any unauthorized transactions on your accounts.
8. Monitor your financial records, statements of accounts, and credit reports for several months after you discover the crime.

# Identify Theft White Paper

## Why should you file a police report?

If you become a victim of identity theft, filing a police report entitles you to legal benefits and advantages that you may not be aware of. The following is a list that includes, but is not limited to, some of these benefits:

1. It entitles you to certain legal rights when it is provided to the three major credit bureaus.
2. It can be used to permanently block fraudulent information that results from identity theft (won't show on your credit reports and records).
3. It prevents the collection of debts that you are not responsible for.
4. It is needed to place an extended fraud alert on your credit report.

## What supervisors should know and do to protect personal information?

Supervisors must maintain a fair balance between protection and business realities while reinforcing flexibility in compliance. Supervisors are required to develop new regulations and procedures that include technical, administrative, and physical safeguards that insure the security and the confidentiality of the employees, students, and external entities.

Such regulations and procedures should be fully consistent with industry standards, protect against anticipated threats to the security and integrity of personal information, and unauthorized access or unauthorized use of information that may result in substantial harm or inconvenience to the employees, students, and external entities including identity theft.

The approach to data security is a risk based approach. Therefore, supervisors must develop, implement, and maintain a “*Comprehensive Information Security Program*” that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the size, scope, and type of business, the amount of resources available, the amount of stored data, and the need for security and confidentiality of students, employees, and external entities.

## Comprehensive information security program

The following is a non exhaustive list that includes, but is not limited to, administrative, technical, and physical safeguards a comprehensive information security program should contain:

1. Ways and methods to identify and assess reasonably foreseeable internal and external risks, strengths, opportunities, weaknesses, and threats t (S.W.O.T) to the security, confidentiality, and integrity of any electronic, paper, or other records containing personal information.
2. Ways and methods to evaluate and improve, where necessary, the effectiveness and efficiency of the implemented administrative, technical, and physical safeguards.

## **Identify Theft White Paper**

3. Reasonable restrictions upon physical access to locked and secured facilities, storage areas, or containers containing electronic, paper, or other records.
4. Tools and ways to monitor the scope of the security measures on a regular basis and whenever there is a potential change in business practices that may reasonably implicate the security or the integrity of records containing personal information.
5. Reasonable steps to select, and by contract retain, third party service providers that are capable to implement and maintain appropriate security measures to protect personal information.
6. Means to detect and prevent security system failures.
7. Designation of one or more employees to maintain the program.
8. Ongoing employee training.
9. Development of security policies for employees relating to the storage access and transportation of records containing personal information outside the business premises.
10. Tools to monitor and enforce employees' compliance with policies and procedures.
11. Progressive or immediate disciplinary measures for violations of the program.
12. Ways to prevent terminated employees from accessing records containing personal information.

### **Computer system security program**

In addition to developing a comprehensive information security program, supervisors also should develop, implement, and maintain a "*Computer System Security Program*" written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are adequate to establish and maintain computer security systems including any wireless systems or online applications that should include, at a minimum and to the extent technically feasible, the following elements:

1. Secure user authentication protocols.
2. Control of user IDs, and other identifiers.
3. Secure methods of assessing and selecting passwords or use of unique identifier technologies.
4. Control of data security passwords to ensure that such passwords are kept in a location and/or format that do not compromise the security of the data they protect.

## **Identify Theft White Paper**

5. Restricting access to active users and active user accounts only.
6. Blocking access to user identification after multiple unsuccessful attempts to gain access.
7. Secure control measures to restrict access to records and files containing personal information to those who need such information to perform their job duties.
8. Assign unique identifications passwords to vendors and third parties.
9. Encryption of all transmitted records and files containing personal information that will travel across public networks or to be transmitted wirelessly.
10. Reasonable monitoring of systems for unauthorized use of, or access to, personal information.
11. Encryption of all personal information stored on laptops on other portable devices.
12. Up-to-date firewall protection and operating system security patches designed to maintain the integrity of the personal information of system or applications connected to the internet.
13. Up-to-date versions of system security agent software which must include malware protection, up-to-date patches, and virus definitions.
14. Education and training of employees on the proper use of the computer security system and the importance of personal information security.

### **What to do in case of a breach of personal information?**

1. Notify law enforcement. Call your local police department and report your situation and the potential risks for identity theft.
2. Consult with your local law enforcement so you do not impede their investigation.
3. Notify the US Postal Inspection Service for incidents involving mail theft.
4. Notify affected employees, students, vendors, businesses and any other external entities.
5. Notify any businesses that you collect or store personal information on their behalf.
6. Notify the major credit bureau if SSN have been stolen as they can facilitate “customer assistance”.
7. Remove the information from your website if the compromise resulted from the improper posting of personal information on your personal or departmental website. Be aware that internet search engines store "cache" information for a period of time.

## Identify Theft White Paper

8. Designate a contact person within your organizations for releasing information.
9. Give the contact person the latest information about the breach, your response, and how individuals should respond.
10. Clearly describe what you know about the compromise. Include how it happened, what information was taken, and if you know how the thieves have used the information, and what actions you have taken already to remedy the situation. Your actions may include but should not be limited to:
  - a. Explaining what response may be appropriate for the type of information taken. For example, people whose SSN has been stolen should contact the major credit bureaus to ask that fraud alerts be placed on their credit reports.
  - b. Providing current information about identity theft (flyers, brochures, newsletters, etc).
  - c. Providing contact information for the law enforcement office working on the case as well as your case number.
  - d. Encouraging those who discover that their personal information has been misused to file a police report and a complaint with the FTC.