

**PENNSYLVANIA**

IDENTITY THEFT RANKING BY STATE: Rank 14, 72.5 Complaints Per 100,000  
Population, 9016 Complaints (2007)  
Updated January 29, 2009

**Current Laws:** A person commits the offense of identity theft of another person if he possesses or uses, through any means, identifying information of another person without the consent of that other person to further any unlawful purpose. Identifying information is defined as “any document, photographic, pictorial or computer image of another person, or any fact used to establish identity, including, but not limited to, a name, birth date, Social Security number, driver’s license number, nondriver governmental identification number, telephone number, checking account number, savings account number, student identification number, employee or payroll number or electronic signature.”

The penalty for identity theft varies based on the value of the property or services obtained by means of the identifying information and the nature of the theft:

- If the total value involved is less than \$2,000, the offense is a misdemeanor of the first degree, punishable by up to five years in prison and/or a fine up to \$10,000.
- If the total value involved is \$2,000 or more, the offense is a felony of the third degree, punishable by up to seven years in prison and/or a fine up to \$15,000.
- Regardless of the total value involved, if the offense is committed in the furtherance of a criminal conspiracy, it is a third degree felony.
- Third or subsequent offenses, regardless of the total value involved, are second degree felonies, punishable by up to ten years in prison and/or a fine up to \$25,000.
- If a person commits an offense against a victim 60 years of age or older or a care-dependent person, the grading of the offense will be one grade higher than generally specified.

Each time a person possesses or uses identifying information constitutes a separate offense. However, the total values involved in offenses under this section committed pursuant to one scheme or course of conduct, whether from the same victim or several victims, may be aggregated in determining the grade of the offense.

The Attorney General has the authority to investigate and institute criminal proceeding for any identity theft violations.

Statute: 18 § 4120

**Jurisdiction:** Any identity theft offense may be deemed to have been committed at any of the following: the place where a person possessed or used the identifying information of another without the other’s consent to further any unlawful purpose; the residence of the person whose identifying information has been lost or stolen or has been used without the person’s consent; or the business or employment address of the person whose identifying information has been lost or

stolen or has been used without the person's consent, if the identifying information at issue is associated with the person's business or employment.

Statute: 18 § 4120

**Police Reports:** A report to a law enforcement agency by a person stating that the person's identifying information has been lost or stolen or that the person's identifying information has been used without the person's consent shall be prima facie evidence that the identifying information was possessed or used without the person's consent.

Statute: 18 § 4120

**Access Devices:** An access device is defined as any card, including, but not limited to, a credit card, debit card and automated teller machine card, plate, code, account number, personal identification number or other means of account access that can be used alone or in conjunction with another access device to obtain money, goods, services or anything else of value or that can be used to transfer funds.

Access device fraud includes using an access device to obtain or in an attempt to obtain property or services with knowledge that: the access device is counterfeit, altered or incomplete; it was issued to another person who has not authorized its use; it has been revoked or canceled; or for any other reason his use of the access device is unauthorized by the issuer or the device holder. The punishment for violations varies based on the value of the property or service obtained or sought to be obtained by means of the access device: If the value is \$500 or more, the offense is a third-degree felony; if the value is \$50 or more but less than \$500, it is a misdemeanor of the first degree; and if it is less than \$50, it is a misdemeanor of the second degree (punishable by up to two years in prison and/or a fine up to \$5,000). Amounts involved in unlawful use of an access device pursuant to a scheme or course of conduct, whether from the same issuer or several issuers, may be aggregated in determining the classification of the offense.

It is third-degree felony to publish, make, sell, give, or otherwise transfer to another, or offer or advertise, or aid and abet any other person to use an access device knowing that it is counterfeit, altered or incomplete, belongs to another person who has not authorized its use, has been revoked or canceled or for any reason is unauthorized by the issuer or the device holder.

Possessing an access device knowing that it is counterfeit, altered, incomplete, or belongs to another person who has not authorized its possession is a third-degree misdemeanor, punishable by up to one year in prison.

For the purposes of these provisions, an actor is presumed to know an access device is counterfeit, altered or incomplete if he has in his possession or under his control two or more counterfeit, altered or incomplete access devices. Any access device fraud offense may be deemed to have been committed at either the place where the attempt to obtain property or services is made, at the place where the property or services were received or provided, or at the place where the lawful charges for said property or services are billed.

Statute: 18 § 4106

**Computer Crimes:** A person commits the offense of unlawful use of a computer if he intentionally and knowingly and without authorization gives or publishes a password, identifying code, personal identification number, or other confidential information about a computer, computer system or database, web site, or telecommunication device. Violations are a third-degree felony.

Statute: 18 § 7611

A person commits the offense of computer trespass if he knowingly and without authority or in excess of given authority uses a computer or computer network with the intent to effect the creation and or alteration of a financial instrument or an electronic transfer of funds. Violations are a third-degree felony.

Statute: 18 § 7615

### **Victim Assistance:**

**Credit Freeze:** All Pennsylvania consumers are allowed to place security freezes on their consumer credit reports to prevent new accounts from being opened in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information. To request a freeze, a consumer must request one in writing by certified mail or through a secure Internet connection if such a connection is made available by the consumer reporting agency. Security freezes may remain in place for up to seven years. Consumer reporting agencies may charge a fee of \$10 to place or temporarily lift a security freeze. However, victims of identity theft with a valid police report or investigative complaint and people 65 years of age or older may not be charged.

The reporting agency must place the freeze within five business days after receiving the request, and within ten days, must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time.

Requests for a temporary unlocking of the freeze must be completed within three business days.

Statute: 45 § 2503

How to Place a Security Freeze in Pennsylvania:

<http://www.consumersunion.org/pdf/security/securityPA.pdf>

**Security Breach:** State law requires state and local governments and individuals and businesses doing business in the state to notify consumers when their unencrypted and unredacted personal information was or is reasonably believed to have been compromised during a security breach, putting them at risk of identity theft. A security breach occurs upon “unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of the Commonwealth.”

An entity must disclose provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the

encryption or if the security breach involves a person with access to the encryption key. Notice must be made without unreasonable delay, consistent with the needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

Personal information is defined as an individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the name and data elements are not encrypted: Social Security number; driver's license number or state identification card number; or a financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. It does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notification can be provided by mail, e-mail, or telephone. If the cost of providing regular notice would exceed \$175,000, the amount of people to be notified exceeds 100,000, or the business does not have sufficient contact information to provide written or electronic notice, substitute notice may be provided. When substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the business's web site, and notification to major statewide media. When a breach involves more than 1,000 people, the entity must also notify the consumer reporting agencies.

Statute: 73 § 2302

**Civil Suits:** Victims of identity theft may file a civil action to obtain actual damages arising from the incident or \$500, whichever is greater, to cover loss of money, reputation or property, whether real or personal. The court may award up to three times the actual damages sustained, but not less than \$500. Victims may also seek reasonable attorney fees and court costs and any additional relief that court deems necessary and proper. The plaintiff must file suit within four years of the date of the offense or from the date of the discovery of the identity theft.

Statute: 42 § 8315

---

### **State Resources:**

“Identity Theft Action Plan” (<http://www.identitythefactionplan.com/>)

- “Identity Theft Action Plan” (<http://www.identitythefactionplan.com/actionplan.pdf>)
- “Prevention Tips” (<http://www.identitythefactionplan.com/preventH.html>)
- “If You’re A Victim of Identity Theft” (<http://www.identitythefactionplan.com/ifYourVictH.html>)

This site directs victims to: “*File a report with your local police department.*” It also explains that victims of criminal identity theft should: “*Contact the arresting or citing law enforcement agency (i.e., the police or sheriff’s department that originally arrested the person using your identity, or the court agency that issued the warrant for the arrest). You’ll need to file an impersonation report to confirm your identity and the police department may take a full set of your fingerprints, your photograph, and copies of any photo identification documents you have including your driver’s license, passport, and Visa.*”

*The law enforcement agency should then recall any warrants and issue a “clearance letter” or certificate of release if you were arrested/booked. **Keep this document with you at all times in case you’re wrongly arrested.** Also, ask the law enforcement agency to file the record of the follow-up investigation establishing your innocence with the district attorney’s office and the court where the crime took place. Ask that the “key name” or “primary name” be changed from your name to the imposter’s name and that your name is noted only as an alias.”*

- “Law Enforcement Related Links ” (<http://www.identitytheftactionplan.com/LawEnforce-H.html>)  
The site also contains information specifically designed to help law enforcement in the fight against identity theft crimes It contains a victim interview checklist, notes the importance of taking a police report, tips on investigating the alleged crime and referring the victim to other law enforcement agencies, and a list of relevant federal and state laws.

Office of the Attorney General, “Identity Theft Toolkit” (<http://www.attorneygeneral.gov/idtheft.aspx?id=1757>)

- “How to Avoid Identity Theft” ([http://www.attorneygeneral.gov/uploadedFiles/Consumers/identity\\_theft.pdf](http://www.attorneygeneral.gov/uploadedFiles/Consumers/identity_theft.pdf))
- “Preventative Actions: Checklist” (<http://www.attorneygeneral.gov/idtheft.aspx?id=1814>)
- “Corrective Actions: Checklist” (<http://www.attorneygeneral.gov/idtheft.aspx?id=1812>)  
This checklist directs victims to: “*File a report with your local police or the police in the community where the identity theft took place. Most credit card issuers and utilities require proof of theft in order to begin the remediation process. Making out a report with your local police is crucial. If, however, the local police tell you that identity theft is not a crime in their jurisdiction, ask to file a Miscellaneous Incident Report in order to memorialize the theft. If they simply will not take a report, see our contact list of [Pennsylvania Sheriffs](#) to file a report with your local sheriff’s department or contact the [Pennsylvania State Police](#).*” Regardless of what entity ultimately takes your complaint, be sure to get a copy of the report or, at the very least, the number of the report, to submit to your creditors and other organizations that may require it.”
- “Corrective Actions: Contact Log” (<http://www.attorneygeneral.gov/idtheft.aspx?id=1818>)
- “Contact List” ([http://www.attorneygeneral.gov/uploadedFiles/Consumers/ID\\_Theft/full\\_contact\\_list.pdf](http://www.attorneygeneral.gov/uploadedFiles/Consumers/ID_Theft/full_contact_list.pdf))  
This document provides contact information for credit reporting agencies, local sheriffs office (to be used if a local police department refuses to take a report), the state police (to be used if the sheriffs office refuses to take a report), and state and federal agencies.
- “Phishing, Pharming, and Call ID Fraud” (<http://www.attorneygeneral.gov/idtheft.aspx?id=1815>)
- “Frequently Asked Questions” (<http://www.attorneygeneral.gov/idtheft.aspx?id=1822>)

---

## **Legislation:**

### **2006:**

**SB 180** allows Pennsylvania consumers to put a security freeze on their credit files to prevent identity thieves from opening new credit accounts in their names. A security freeze enables a

consumer to prevent anyone from looking at his or her own credit reporting file for purposes of granting credit unless the consumer chooses to let that particular business look at the information. This gives consumers control over who has access to their information needed to process a credit application and effectively prevents others from opening new accounts in their name. When the consumer is applying for credit, the security freeze can be lifted temporarily so the application can be processed.

**2005:**

**SB 712** requires state and local government agencies and businesses to notify individuals when a security breach results in their personal information being released by unauthorized parties and causes or will cause loss or injury to a Pennsylvania resident.

**2002:**

**HB 1546** expands the offense of identity theft to include any possession or use of personal identification without consent for an unlawful purpose. The law also allows for separate offenses to be linked in one scheme in order to help determine the grade of the offense. An action relating to damages in actions for identity theft may be brought within four years of the date of the offense, or four years from the date of the discovery of the identity theft. Damages include actual damages arising from the incident or \$500, whichever is greater. Reasonable attorney fees and court costs also may be awarded, as well as any additional relief the court deems necessary and proper.