ID Safety
Protecting the *real* you, and *only* you.

In partnership with: INTERNATIONAL ASSOCIATION of CHIEFS OF POLICE Bank of America

MASSACHUSETTS
IDENTITY THEFT RANKING BY STATE: Rank 23, 66.5 Complaints Per 100,000 Population, 4292 Complaints (2006)
Updated January 17, 2009

Current Laws:
Identity Crime: A person is guilty of identity fraud if he, with intent to defraud, poses as another person without the express authorization of that person and uses such person's personal identifying information to obtain or to attempt to obtain money, credit, goods, services, anything of value, any identification card or other evidence of such person's identity, or to harass another. Violations are punishable by a fine up to $5,000 and/or imprisonment for up to 2 ½ years.

A law enforcement officer may arrest without a warrant any person he has probable cause to believe has committed the offense of identity fraud as defined in this section.

"Personal identifying information" means any name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number or computer password identification.
Statute: 266 § 37E: http://www.mass.gov/legis/laws/mgl/266-37e.htm

Payment Cards: A person is guilty of misuse of a credit card if he:

- Makes or causes to be made, either directly or indirectly, any false statement as to a material fact in writing, knowing it to be false, and with intent that it be relied on, respecting his identity or that of any other person for the purpose of procuring the issuance of a credit card.
- Takes a credit card from the person, possession, custody or control of another without the cardholder's consent, or who, with knowledge that it has been so taken, receives the credit card with intent to use it, sell it, or transfer it to a person other than the issuer or cardholder.
- Receives a credit card that he knows to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder, and who retains possession with intent to use it or to sell it or to transfer it to a person other than the issuer or the cardholder.
- Being a person other than the issuer or his authorized agent, sells a credit card, or buys a credit card from a person other than the issuer or his authorized agent.
- Uses, for the purpose of obtaining money, goods, services or anything else of value, a credit card obtained or retained fraudulently, or a credit card which he knows is forged, expired or revoked, where the value of money, goods or services obtained is less than $250.

Violations are punishable by a fine up to $500 and/or up to one year in jail.
Statute: 266 § 37B: http://www.mass.gov/legis/laws/mgl/266-37b.htm

If the value of the goods, money, services, or anything else of value is over $250, a person is guilty of fraudulent use of a credit card, punishable by up 2 ½ to 5 years in prison and/or a fine of up to $2000.
Statute: 266 § 37C: http://www.mass.gov/legis/laws/mgl/266-37c.htm

Disposal of Records: State law restricts how businesses can dispose of paper records with confidential information about individuals. The law will prohibit businesses from knowingly discarding paper records or documents with personal information without first redacting the data or shredding or otherwise destroying the documents. Electronic media must be destroyed or erased so that the personal information cannot practicably be read or reconstructed. It will apply to data that includes a person's name and Social Security, driver's license and financial account or credit or debit car numbers.
Statute: 93I § 1-3: http://www.mass.gov/legis/laws/mgl/gl-93i-toc.htm

Victim Assistance:

Mandatory Police Reports: Law enforcement officers are required to accept a police incident report from an identity theft victim, and provide a copy of the report to the victim upon request within 24 hours. The incident report may be filed in any county where a victim resides; or in any county where the owner or license holder of personal information stores or maintains the personal information; the owner or license holder's principal place of business or any county in which the breach of security occurred.
Statute: 266 § 37E: http://www.mass.gov/legis/laws/mgl/266-37e.htm

Restitution: A person found guilty of identity fraud will be ordered to make restitution for financial loss sustained by a victim as a result of the violation. Financial loss may include any costs incurred by the victim in correcting his/her credit history or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt or other obligation, including lost wages and attorney's fees.
Statute: 266 § 37E: http://www.mass.gov/legis/laws/mgl/266-37e.htm

Protection of Personal Information: This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth is required to develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. This security program must be reasonably consistent with industry standards, and must contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. The regulations require each information security program to include:

- Designating one or more employees to maintain the comprehensive information security program;
- Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks.

- Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
- Imposing disciplinary measures for violations of the comprehensive information security program rules.
- Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.
- Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information.
- Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.
- Reasonable restrictions upon physical access to records containing personal information;
- Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
- Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

The regulations also require the establishment and maintenance of a security system covering computers with, at a minimum:

- Secure user authentication protocols;
- Secure access control measures;
- Where technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks or be transmitted wirelessly;
- Reasonable monitoring of systems, for unauthorized use of or access to personal information;
- Encryption of all personal information stored on laptops or other portable devices;
- For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions
- Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Regulation: 201 CMR 17.00:
http://www.mass.gov/?pageID=ocaterminal&L=3&L0=Home&L1=Consumer&L2=Identity+Theft&sid=Eoca&b=terminalcontent&f=idtheft_201cmr17&csid=Eoca

Security Breach: State law requires state and local government agencies and individuals and businesses doing business in the state to notify residents when their 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 is defined as the "unauthorized acquisition or unauthorized use of unencrypted data, or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity or personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth."

Notice must be provided as soon as practicable and without unreasonable delay when a person or agency that owns or licenses personal information knows or has reason to know of a breach of security, or when the person or agency knows or has reason to know that the personal information of a resident was acquired or used by an unauthorized person or used for an unauthorized purpose. Notice must also be made to the Attorney General, the Director of Consumer Affairs and Business Regulation, and the consumer reporting agencies. The notice provided to residents must include, but is not limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies.

Personal information is defined as a resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident: Social Security number; driver's license number or state-issued identification card number; or a financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number (PIN), or password that would permit access to a resident'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 or e-mail. If the cost of providing regular notice would exceed $250,000, the amount of people to be notified exceeds 500,000, or the person or agency 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, clear and conspicuous posting on the home page of the person or agency if they maintain a web site, and publication in or broadcast through media that provides notice throughout the state.
Statute: 93H § 1-6: http://www.mass.gov/legis/laws/mgl/gl-93h-toc.htm

Security Freeze: All Massachusetts 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 mail. Consumer reporting agencies may charge a fee of $5 to place or temporarily lift a security freeze. However, victims of identity theft or his/her spouse with a valid police report relating to the identity theft may not be charged.

The reporting agency must place the freeze within three business days after receiving the request, and within five business 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: 93 § 62A: http://www.mass.gov/legis/laws/mgl/93-62a.htm

---

State Resources:

Office of the Attorney General, "Identity Theft" (http://www.mass.gov/?pageID=cagosubtopic&L=4&L0=Home&L1=Consumer+Protection&L2=Scams+and+Identity+Theft&L3=Identity+Theft&sid=Cago)

"Attorney General's Guide to ID Theft for Victims and Consumers" (http://www.mass.gov/Cago/docs/Consumer/identity_theft_022708.pdf)
This document directs victims to: "*Promptly make a report with your local police department. File a police report with your local police department, keep a copy for yourself, and give a copy to your creditors and their credit bureaus.*"

"Understanding Identity Theft" (http://www.mass.gov/?pageID=cagoterminal&L=4&L0=Home&L1=Consumer+Protection&L2=Scams+and+Identity+Theft&L3=Identity+Theft&sid=Cago&b=terminalcontent&f=consumer_understanding_id_theft&csid=Cago)

"First Step for Victims" (http://www.mass.gov/?pageID=cagoterminal&L=4&L0=Home&L1=Consumer+Protection&L2=Scams+and+Identity+Theft&L3=Identity+Theft&sid=Cago&b=terminalcontent&f=consumer_first_steps_for_victims&csid=Cago)

"Security Freezes and Fraud Alerts" (http://www.mass.gov/?pageID=cagoterminal&L=4&L0=Home&L1=Consumer+Protection&L2=Scams+and+Identity+Theft&L3=Identity+Theft&sid=Cago&b=terminalcontent&f=consumer_security_freeze_fraud_alert&csid=Cago)

"Reporting Identity Theft" (http://www.mass.gov/?pageID=cagoterminal&L=4&L0=Home&L1=Consumer+Protection&L2=Scams+and+Identity+Theft&L3=Identity+Theft&sid=Cago&b=terminalcontent&f=consumer_reporting_id_theft&csid=Cago)
"*File a police report with your local police department, keep a copy for yourself, and give a copy to your creditors and the credit bureaus. Massachusetts law provides that identity theft is a crime (M.G.L. c. 266, s. 37E). You should be aware that not all identity theft complaints can or will be investigated. However, by providing law enforcement offices with a written report, you make it possible for law enforcement offices to spot trends and patterns, and to identify the prevalence of identity theft. "*

Office of Consumer Affairs and Business Regulation, "Surviving Theft of Financial Identity" (http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=surviving_theft_of_financial_identity&csid=Eoca)
This site directs victims to: "*File a police report and criminal complaint with your local police department and/or district attorney's office. Theft of financial identity is a criminal act in Massachusetts punishable by a fine of up to $5,000 and/or up to two and a half years in jail and restitution of financial loss to the victim. In addition, law enforcement may use the federal Identity Theft and Assumption Deterrence Act of 1998 to prosecute identity imposters. Be sure to keep a copy of your filed complaint, as some creditors may request it for verification of your case.*"

Office of Public Safety, "Identity Theft" (http://www.mass.gov/?pageID=eopssubtopic&L=3&L0=Home&L1=Crime+Prevention+%26+Personal+Safety&L2=Identity+Theft&sid=Eeops)
This site contains information on identity theft, ways to prevent the crime, and what to do if you become a victim of identity theft.

"What Should You Do If You Become a Victim of Identity Theft" (http://www.mass.gov/?pageID=eopsterminal&L=3&L0=Home&L1=Crime+Prevention+%26+Personal+Safety&L2=Identity+Theft&sid=Eeops&b=terminalcontent&f=msp_divisions_investigative_services_identity_theft_msp_identity_theft_what_should_victim_do&csid=Eeops)

Massachusetts Registry of Motor Vehicles, "Information About Compromised Identity Data" (http://www.mass.gov/rmv/tjx.htm)
This site recommends that if your personal information has been compromised, you should change your license number immediately if you are currently using a Social Security Number as your license number. It explains how to change your license of identification card number, and how to place an activity hold on your driver's license, which prevents all future license transactions in the state.

"Identity Theft Forms" (http://www.mass.gov/rmv/forms/identity_theft.htm)

Massachusetts Association of Chiefs of Police, "Identity Theft" (http://www.masschiefs.org/page.php?pageid=65)
This site explains that: "*Most Massachusetts police departments ascribe to a policy drafted by the Massachusetts Chiefs of Police Association in conjunction with the Massachusetts Bankers Association and the US Postal Inspection Service. The basic tenets of the policy are:*

- *A victim of identity theft can report the crime to their local police department, even if the offense did not actually occur there. Identity theft crosses state and even national borders, and it is extremely important that the theft is reported quickly, so most Massachusetts police chiefs have decided to take reports from their citizens even when they do not have jurisdiction to prosecute the underlying offenses.*
- *If a financial transaction can be identified in another jurisdiction, the investigating officer will make a formal referral to the appropriate law enforcement agency.*
- *Police officers and detectives from your local police department thoroughly investigate all*

crimes related to identity crime occurring in your community.

- *Financial institutions often ask victims to send them a police report, so your local police department normally provides a copy of the report to the victim once it has been reviewed and approved. It can be mailed to you or you can pick it up at the police station.*
- *All reports about identity theft are faxed to the Identity Theft and Financial Crimes Task Force in Boston. The task force assists police departments and maintains a database of identity crimes occurring in New England. Where appropriate, the task force notifies and coordinates their investigations with the US Secret Service.*
- *Most officers investigating a case of identity theft will provide the victim with a Resource Guide, or you can obtain the same information from our web site by clicking on "If you have been a victim …". The guide lists steps the victim can take to minimize the damage done by the crime, such as notifying a credit bureau and financial institutions, and registering the case on the FTC web site.*
- *The guide and information on our web site also explains how victims can notify the Social Security Administration if their social security number has been compromised.*
- *Cases that need follow-up investigation are often referred to the detectives of your police department. Detectives coordinate investigations with the task force, or follow up on fraudulent transactions occurring in your community that have been referred by other law enforcement agencies.*
- *Criminals committing crimes related to identity theft are often recorded by security cameras. Detectives post those photographs on the http://www.massmostwanted.org website. Check the web site out to view photographs of people committing identity theft and other crimes."*

Legislation:

2008:

The Massachusetts Office of Consumer Affairs and Business Regulation issued new rules that require businesses to better safeguard consumers' personal information. The regulations require companies that handle personal information such as credit card accounts and Social Security numbers to encrypt data stored on laptops, monitor employee access to data, and take other steps to protect customer information. Governor Deval Patrick also signed an executive order that requires state agencies to take similar measures.

2007:

Lawmakers passed comprehensive legislation (**HB 4144**) to protect consumers from identity theft. The bill:

- Requires businesses and government agencies to protect consumers' information to avoid a security breach.
- Requires commercial entities and government agencies to notify affected consumers if their personal identifying information has been lost or stolen, putting them at risk of identity theft.
- Allows consumers to place a security freeze on their credit reports, preventing identity thieves from taking out credit in their name.
- Requires that documents containing personal identifying information be properly disposed of so that the information cannot be practicably read.
- Allows a victim of identity theft to obtain a copy of their credit report from any law enforcement agency, even if the crime did not occur in that jurisdiction.