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

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

MAINE
IDENTITY THEFT RANKING BY STATE: Rank 45, 40.2 Complaints Per 100,000 Population, 530 Complaints (2007)
Updated December 16, 2008

Current Laws: A person is guilty of misuse of identification if, in order to obtain confidential information, property or services, the person intentionally or knowingly:

- Presents or uses a credit or debit card that is stolen, forged, canceled, or obtained as a result of fraud or deception.
- Presents or uses an account, credit or billing number that that person is not authorized to use or that was obtained as a result of fraud or deception.
- Presents or uses a form of legal identification that that person is not authorized to use. "Legal identification" includes a Social Security card, Social Security number, birth certificate, driver's license, government-issued identification card, oral statement of full name and date of birth, or any other means of identifying a person that is generally accepted as accurate and reliable.

Misuse of identification is a Class D crime, punishable by up to a year in jail and/or a $2000 fine.
Statute: 17A§905-A: http://janus.state.me.us/legis/statutes/17-A/title17-Asec905-A.html

Scanning Device: It is illegal to use a scanning device or a reencoder without the permission of the authorized payment card user whose card information is scanned or reencoded and with the intent to defraud or deceive the authorized payment card user, the issuer of the authorized payment card user's payment card or another person. A reencoder is an electronic device that places encoded information from the computer chip or magnetic strip or stripe of a payment card onto the computer chip or magnetic strip or stripe of another payment card or any electronic medium that allows an authorized transaction to occur. A scanning device means a scanner, reader or any other electronic device that is used to access, read, scan, obtain, memorize or store, temporarily or permanently, information encoded on the computer chip or magnetic strip or stripe of a payment card. Misuse of a scanning device or reencoder is a Class D crime.
Statute: 17A§905-B: http://janus.state.me.us/legis/statutes/17-A/title17-Asec905-B.html

Victim Assistance:

Mandatory Police Reports: A person who knows or reasonably believes that the person's personal information has been misused may report the misuse and obtain a police report by contacting the local law enforcement agency that has jurisdiction over the person's actual residence or place of business. That law enforcement agency must make a police report of the matter and provide the complainant with a copy of that report. At its discretion, the law enforcement agency may undertake an investigation of the matter or refer it to another law enforcement agency. If the suspected crime was committed in a jurisdiction outside of the state,

the local law enforcement agency must refer the report to the law enforcement agency where the suspected crime was committed.
Statute: 10§1350-B: http://janus.state.me.us/legis/ros/lom/LOM123rd/123S1/PUBLIC634.asp

Security Freeze: State law allows all consumers to place security freezes on their consumer credit reports to prevent identity thieves from opening new accounts 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 to the credit reporting agencies. The agency may charge up to $10 to place, lift, or temporarily lift a security freeze. In addition, it may charge $12 to lift the freeze for one particular creditor. However, the credit reporting agency may not charge identity theft victims who provide a police report.

The reporting agency must place the freeze within five business days after receiving the request, and within ten 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: 10§1313-C: http://janus.state.me.us/legis/statutes/10/title10sec1313-c.html
How to Place a Security Freeze: www.consumersunion.org/pdf/security/securityME.pdf

Credit Block: If a security freeze is in place, a consumer reporting agency must expunge any information in the file of a consumer that resulted from identity theft.
Statute: 10§1313-D: http://janus.state.me.us/legis/statutes/10/title10sec1313-D.html

Security Breaches: State law requires state government agencies, businesses operating in the state, and private and public universities that collect and maintain computerized records containing consumers' personal information to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. A security breach is defined as the "unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person."

Personal information includes a individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not redacted or encrypted: Social Security number; driver's license number or state identification card number; account number or credit or debit card number if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; account passwords or personal identification numbers or other access codes; or any of the data elements when not in connection with the individual's name if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. Publicly available information is not included.

Entities must conduct reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. It must give notice of a breach following discovery or notification to any resident whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. Disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity, security, and confidentiality of the data in the system.

Notification can be provided to the affected persons by mail or e-mail. If the cost of providing regular notice would exceed $5,000, the amount of people to be notified exceeds 1,000, or the person does not have sufficient contact information, substitute notice may be provided. When substitute notice is used, it should consist of the following, as applicable: e-mail notice, conspicuous posting on the person's publicly accessible web site, and notification to major statewide media. If notice is provided to more than 1000 residents, the consumer reporting agencies and appropriate state regulators must also be notified.
Statute: 10§1348: http://janus.state.me.us/legis/statutes/10/title10sec1348.html

---

State Resources:

Office of the Attorney General: "Identity Theft"
(http://www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml)
This site directs victims to: "*Report the crime immediately to local law enforcement. Make sure a written report is taken and that you receive a copy of the police report so that you can give copies to creditors. If local law enforcement will not give you a copy of your report, contact the Attorney General at 626-8800."*

Office of the Secretary of State: "Protect Your Privacy & Prevent Identity Fraud"
(http://www.maine.gov/sos/IDFraud.htm)
The document directs victims of identity theft to take four steps, the first of which is: "*Contact your local Police Department*."

Bureau of Financial Institutions: "Credit Reports and Identity Theft"
(http://www.maine.gov/pfr/financialinstitutions/consumer/credit_report.htm)

Department of Professional and Financial Regulation, Consumer Credit Protection, "Identity Theft" (www.maine.gov/pfr/consumercredit/documents/identity_theft.htm)

Legislation:

2008:
Under **LD 2220,** a person who knows or reasonably believes that his personal information has been misused may report the misuse and obtain a police report by contacting the local law enforcement agency that has jurisdiction over the person's actual residence or place of business. That law enforcement agency must make a police report of the matter and provide the

complainant with a copy of that report. At its discretion, the law enforcement agency may undertake an investigation of the matter or refer it to another law enforcement agency. If the suspected crime was committed in a jurisdiction outside of the state, the local law enforcement agency must refer the report to the law enforcement agency where the suspected crime was committed.

2006:

LD 2017 expands the state's law requiring notice of security breaches that could result in the unauthorized release of personal data. Previously, the law applied only to "information brokers," companies that purchase personal information for marketing purposes. The new law strikes all references to information brokers and replaces it with "person" so the law now applies to any entity or individual, including the state. As a result, state agencies, private and state schools and universities, and businesses are now all required to notify consumers if the misuse of information has occurred or if it is reasonably possible that misuse will occur. The bill also establishes a private cause of action for certain violations of the obligation to notify consumers.

LD 1834 clarifies the process of cleaning up credit reports of identity theft victims. Under the bill, if a security freeze is in place, a consumer reporting agency must expunge any information in the file of a consumer that resulted from identity theft.

2005:

LD 1671 requires companies that gather personal information to disclose publicly when a security breach may result in the authorized release of data. The law applies only to information brokers, namely companies that purchase personal information for marketing purposes.

LD 581 allows consumers to freeze their credit reports when they learn they have been victimized by identity theft. It prohibits a consumer reporting agency from furnishing a consumer report or disclosing information about a consumer unless the consumer has authorized the disclosure if the consumer has given a copy of a police report to the consumer reporting agency that was prepared by a law enforcement agency in investigation of identity theft involving the consumer.

LD 85 prohibits the use of a scanning device or reencoder to obtain or record encoded information from the magnetic strip of a payment card without permission of the cardholder to defraud the authorized cardholder, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a credit card. A reencoder is an electronic device that places encoded information from the magnetic strip or stripe of a credit card onto the magnetic strip or stripe of a different card. Misuse of a scanning device or reencoder is a Class D crime.