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

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

NEW HAMPSHIRE
IDENTITY THEFT RANKING BY STATE: Rank 37, 48.9 Complaints Per 100,000 Population, 643 Complaints (2007)
Updated January 17, 2009

Current Laws: A person is guilty of identity fraud when he/she:

- Poses as another person with the purpose to defraud in order to obtain money, credit, goods, services, or anything else of value;
- Obtains or records personal identifying information about another person without the express authorization of such person, with the intent to pose as such person;
- Obtains or records personal identifying information about a person without the express authorization of such person in order to assist another to pose as such person; or
- Poses as another person, without the express authorization of such person, with the purpose of obtaining confidential information about such person that is not available to the general public.

Identity fraud is a class A felony, punishable by up to 15 years in jail and/or a $4,000 fine.
Statute: §638-26: http://www.gencourt.state.nh.us/rsa/html/LXII/638/638-26.htm

"Personal identifying information" is defined as any name, number, or information 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, employer or place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number, debit card number, personal identification number, account number, or computer password identification.
Statute: §638-25: http://www.gencourt.state.nh.us/rsa/html/LXII/638/638-25.htm

State law prohibits any person, without the authorization, consent, or permission of the other person, to do any of the following, with fraudulent intent:

- Obtain, record, or access personal information or a financial device that would assist the person in accessing financial resources or obtaining personal information owned by the other person other than that which is necessary to process a transaction for the benefit of the other person;
- Obtain goods, services, or some other benefit through the use of personal information or a financial device of the other person;
- Obtain personal information or financial device documents in the other person's name;
- Possess the personal information or a financial device of the other person without permission or lawful authority, with the intent to use or to aid or permit some third person to use such information or device to obtain cash, credit, property, services, or any other thing of value or to make a financial payment;
- Use or possess personal information or a financial device of the other person without permission or lawful authority with the intent to obtain, or to aid or permit some third person to obtain, a government-issued document;

- Falsely make, complete, or alter a written instrument containing any personal information of the other person; or
- Make or convey a materially false statement, without permission or lawful authority, with the intent to obtain, record, or access the personal information or financial device of the other person.

"Financial device" means any instrument or device that can be used to obtain cash, credit, property, services, or any other thing of value or to make financial payments, including but not limited to any of the following: a credit card, banking card, debit card, electronic fund transfer card, or guaranteed check card; a check; a negotiable order of withdrawal; a share draft; a money order; an automated clearing house or other electronic transaction; or any device or process used to transfer value from one person or entity to another.

"Personal information" includes any one or more of the following, whether the information is owned by or assigned to the person it relates to: a first and last name of a user, whether given at birth or adoption, assumed, or legally changed; a home or physical address; a telephone number; a Social Security number; a personal identification number; a credit or debit card number; any access code associated with a credit or debit card; a date of birth, birth certificate number, or place of birth; a password or access code; a financial institution account number; or a driver's license or other governmental identification.

These provisions do not apply when a person obtains the identity of another person to misrepresent his or her age for the sole purpose of obtaining alcoholic beverages, tobacco, or another privilege denied to minors.
Statute: §359-I: http://www.gencourt.state.nh.us/rsa/html/xxxi/359-i/359-i-mrg.htm

Payment Cards: A person is guilty of fraudulent use of a credit card if he uses a credit card for the purpose of obtaining property or services with knowledge that the card is stolen; has been revoked or cancelled; or the use is unauthorized by either the issuer or the person to whom the credit card is issued. It is a class A felony (punishable by up to 15 years in jail and/or a $4,000 fine) if the value of the property or services obtained is over $1000, a class B felony (punishable by up to 7 years in jail and/or a fine of $4,000) if between $500 and $1000, and a misdemeanor if the value is under $500.
Statute: §638:5: http://www.gencourt.state.nh.us/rsa/html/LXII/638/638-5.htm

Scanning Devices: A person is guilty of the crime of using a scanning device or reencoder to defraud when the person knowingly:
- Uses a scanning device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card without the permission of the authorized user of the payment card and with the intent to defraud the authorized user, the issuer of the authorized user's payment card, or a merchant; or
- Uses a reencoder to place information encoded on the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card without the permission of the authorized user of the card from which the information is being reencoded and with the intent to defraud the authorized user, the issuer of the authorized user's payment card, or a merchant.

Violations are a misdemeanor, unless the person used a scanning device or reencoder to defraud two or more times, in which case it is a class B felony, punishable by up to 7 years in jail and/or a $4,000 fine. Second or subsequent offenses are also a class B felony.
Statute: §638:29: http://www.gencourt.state.nh.us/rsa/html/LXII/638/638-29.htm

Spyware: State law prohibits the use or installation of spyware, software that either employs a user's Internet connection in the background without his/her knowledge or permission; sends information about the computer's usage to a remote computer or server or displays or causes to be displayed an advertisement in response to the computer's usage; or sends or causes to be sent personal information residing on the computer to a remote computer or server. A person who uses or installs spyware is guilty of a class A misdemeanor, punishable by up to one year in prison and/or a $2,000 fine.
Statute: §359-H:1 through H:6: http://www.gencourt.state.nh.us/rsa/html/NHTOC/NHTOC-XXXI-359-H.htm (Index of Section)

Victim Assistance:
Restitution: In addition to any criminal penalties, people convicted of identity fraud will be ordered to make restitution for economic loss sustained by a victim as a result of such violation.
Statute: §638-26: http://www.gencourt.state.nh.us/rsa/html/LXII/638/638-26.htm

Civil Suits: Identity theft victims may bring an action in his or her county of residence or any county in which any part of the act took place, regardless of whether the person who committed the violation was ever actually present in that county, against the person who violated this chapter to recover $5,000 for each incident, or three times the actual damages, whichever is greater, and reasonable attorney's fees and court costs.
Statute: §359-I: http://www.gencourt.state.nh.us/rsa/html/xxxi/359-i/359-i-mrg.htm

Court Orders: A victim may use any conviction for identity theft or any court order received in a civil suit as a submission to any governmental entity or private business as proof that any financial accounts were created or altered unlawfully and were not the actions of the victim.
Statute: §359-I: http://www.gencourt.state.nh.us/rsa/html/xxxi/359-i/359-i-mrg.htm

Mandatory Police Report: A person who has learned or reasonably suspects that he or she has been the victim of identify theft may contact the local law enforcement agency that has jurisdiction over his or her place of residence, which must take a police report of the matter, and provide the complainant with a copy of that report. If the jurisdiction for investigation and prosecution lies elsewhere, the agency may refer the complaint to the law enforcement agency in a different jurisdiction. A complaint filed under this section is not required to be counted as an open case for purposes such as compiling open case statistics.
Statute: §359-B:29: http://www.gencourt.state.nh.us/rsa/html/XXXI/359-B/359-B-29.htm

Security Freeze: State law allows all New Hampshire residents 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. A credit reporting agency may charge up to $10 to place or temporarily unlock the freeze, although there is no charge for victims of identity theft with a valid police report or other complaint.

The reporting agency must place the freeze within five business days after receiving the request, and within ten days of placing the freeze must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used when providing authorization for the release of credit information for a specific party or period of time. Requests for a temporary unlocking of the freeze must be completed within three business days.
Statute: §359-B-23 through B-26: http://www.gencourt.state.nh.us/rsa/html/NHTOC/NHTOC-XXXI-359-B.htm (Index of section)

Credit Freeze Fact Sheet: http://doj.nh.gov/consumer/credit_freeze.html.
How to Place a Credit Freeze: http://www.consumersunion.org/pdf/security/securityNH.pdf

Security Breach: State law requires any person doing business in the state who owns or licenses computerized data that includes personal information to, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person must notify the affected individuals as soon as possible. Notification may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security. A security breach occurs upon "unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state."

Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted: Social Security number; driver's license number or other government identification number; or account 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. Publicly available information is not included.

Notification can be provided to the affected persons by mail, e-mail, or by telephone, and must include a description of the incident in general terms; the approximate date of breach; the type of personal information obtained as a result of the security breach; and the telephonic contact information of the person subject to this section. 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 must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the business or agency's web site, and notification to major statewide media. In addition, notification must be made to the appropriate state regulatory agency, depending on the type of business. If more than 1,000 consumers are to be notified, the person must also notify the consumer reporting agencies.
Statute: §359-C-20: http://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-20.htm

Free Credit Report: State law requires a consumer credit reporting agency to provide an identity theft victim with free copies of his/her consumer credit report upon request, if the victim provides a police report, investigative report, or complaint the consumer has filed with a law enforcement agency about unlawful use of personal information by another person.
Statute: 359-B:27: http://www.gencourt.state.nh.us/rsa/html/XXXI/359-B/359-B-27.htm

---

State Resources:

Office of the Attorney General, "Identity Theft"
(http://doj.nh.gov/consumer/sourcebook/identity.html)
This document instructs victims to: "*File a police report. You can file with your local police or with the police where the fraudulent activity took place. For example, you live in Derry, but the address given by the thief is Manchester, so you could file a report in Manchester or Derry. Get a copy of the police report just in case a bank or credit card company needs proof of the crime at a later date. This can also help you in dealing with debt collectors*."

"Identity Theft Protection Toolkit" (http://doj.nh.gov/consumer/pdf/protection_kit.pdf)
This document directs victims to: "*Report the incident to law enforcement. Contact your local police department or sheriffs office to file a report. When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit. Request a copy of the police report. Some creditors will request to see the report to remove the debts created by the identity thief*."

"Identity Theft Complaint Form" (http://www.egov.nh.gov/identity-theft/pdftrans.pdf)
"Report Identity Theft Electronically" (https://www.egov.nh.gov/identity-theft/step1.asp)

"Credit Report Freeze" (http://doj.nh.gov/consumer/credit_freeze.html)

Legislation:

2007:
HB 227 prohibits any person, without the authorization, consent, or permission of the other person, to do any of the following, with fraudulent intent:

- Obtain, record, or access personal information or a financial device that would assist the person in accessing financial resources or obtaining personal information owned by the other person other than that which is necessary to process a transaction for the benefit of the other person;
- Obtain goods, services, or some other benefit through the use of personal information or a financial device of the other person;
- Obtain personal information or financial device documents in the other person's name;
- Possess the personal information or a financial device of the other person without permission or lawful authority, with the intent to use or to aid or permit some third person to use such information or device to obtain cash, credit, property, services, or any other thing of value or to make a financial payment;

- Use or possess personal information or a financial device of the other person without permission or lawful authority with the intent to obtain, or to aid or permit some third person to obtain, a government-issued document;
- Falsely make, complete, or alter a written instrument containing any personal information of the other person; or
- Make or convey a materially false statement, without permission or lawful authority, with the intent to obtain, record, or access the personal information or financial device of the other person.

The bill also permits a victim of identity theft to bring a private action for damages and to use the judgment to correct related public and private records.

2006:

SB 334 grants consumers the right to place a security freeze on their credit reports to prevent an identity thief from opening an account or obtaining credit under their name. Credit freezes will be provided at no cost to victims of identity theft who submit a police report, investigative report, or complaint filed with a law enforcement agency about the unlawful use of personal information by another person. All other consumers can be charged $10 to place a freeze, and $10 each time the freeze is lifted.

The bill also requires police departments to take a police report from people who have learned or reasonably suspect that they are victims of identity theft. They must also provide a copy of the report to the complainant. If the identity theft occurred in another jurisdiction, the agency can refer it to the appropriate law enforcement agency with jurisdiction over investigation and prosecution.

In addition, the bill requires that victims of identity theft receive free credit reports from the reporting agencies.

HB 1660 requires businesses operating in the state to disclose security breaches to affected consumers. A security breach is defined as the unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a business. In this case, personal information means an individual's first name or initial and last name, in combination with a Social Security number, driver's license number, or account number, credit or debit card number, in combination with any required security code, access code, or password that permit access to an individual's financial account.

The notice can be delayed if law enforcement decides that disclosure of the breach would impede a criminal investigation. The notice can be mailed, e-mailed, or given by phone. If contact information is not available, more than 1,000 people were affected by the breach, or if providing notification would cost more than $5,000, substitute forms of notice may be given, including posting a notice on a website and notifying major statewide media.

2005:
HB 47 makes it a class A misdemeanor to use spyware to knowingly alter, take control of, or damage a person's computer or Internet access. It also prohibits using spyware to obtain personal data from a computer.

2004:
SB 521 increases the penalty for identity fraud to a class A felony in all cases. Previously, this only applied to cases where the property or damages received exceeded $1000.

2003:
SB 149 prohibits the use of a scanning device or reencoder that is used to obtain or record encoded information from the magnetic strip of a payment card. Scanning devices are defined as 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 magnetic strip or stripe of a payment card. A re-encoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are a misdemeanor, unless the person used a scanning device or reencoder to defraud two or more times, in which case it is a class B felony, punishable by up to 7 years in jail and/or a $4,000 fine. Second or subsequent offenses are also a class B felony.