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

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

RHODE ISLAND
IDENTITY THEFT RANKING BY STATE: Rank 34, 56.0 Complaints Per 100,000 Population, 592 Complaints (2007)
Updated January 5, 2009

Current Laws: A person commits the crime of identity fraud if he knowingly:

- Produces an identification document or a false identification document without lawful authority;
- Transfers an identification document or a false identification document knowing that the document was stolen or produced without lawful authority;
- Possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor) or false identification documents;
- Possesses an identification document (other than one issued lawfully for the use of the possessor) or a false identification document, or financial information with the intent that the document or financial information be used to defraud the United States, the State of Rhode Island, any political subdivision of it or any public or private entity;
- Transfers or possesses a document-making implement with the intent that the document-making implement will be used in the production of a false identification document or another document-making implement which will be so used;
- Possesses a false identification document that is or appears to be a genuine identification document of the United States, the State of Rhode Island or any political subdivision of it or any public or private entity which is stolen or produced without lawful authority knowing that the document was stolen or produced without such authority; or
- Transfers or uses with intent to defraud, without lawful authority, a means of identification or financial information of another person living or dead, with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal, state or local law.

"Means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

- Name, Social Security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code; or
- Telecommunication identifying information or access device.

"Financial information" means any of the following information identifiable to an individual that concerns the amount and/or condition of an individual's assets, liabilities or credit: account numbers and balances; transactional information concerning any account; or codes, passwords,

Social Security numbers, tax identification numbers, driver's license numbers or any other information held for the purpose of account access or transaction initiation.

These provisions do not apply to a person under 21 who misrepresents or misstates his age through the presentation of any document in order to enter any premises licensed for the retail sale of alcoholic beverages for the purpose of purchasing or attempting to purchase alcoholic beverages.

Violations are a felony, punishable by up to three years in prison and/or a fine up to $5000 for a first conviction. Second convictions are punishable by three to five years in prison and/or a fine up to $10,000; and third or subsequent convictions will result in five to ten years in prison and/or a fine up to $15,000.
Statute: §11-49.1: http://www.rilin.state.ri.us/Statutes/TITLE11/11-49.1/INDEX.HTM

Payment Cards: A person is guilty of obtaining a credit card through fraudulent means if he:

- 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, sell, or transfer it to a person other than the issuer or the 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, sell, or transfer it to a person other than the issuer or the cardholder;
- If not the issuer, sells a credit card, or buys a credit card from a person other than the issuer;
- If not the authorized cardholder, signs a credit card with the intent to defraud the issuer or a person or organization providing money, goods, services, or anything else of value; or
- Receives two or more credit cards issued in the name or names of different cardholders, which he has reason to know were taken or retained under circumstances that constitute credit card theft.

Violations are punishable by up to one year in jail and/or a fine up to $1000, with the exception of receiving two or more credit cards issued in the name of different cardholders, which is punishable by up to three years in prison and/or a fine up to $3000.
Statute: §11-49-3: http://www.rilin.state.ri.us/Statutes/TITLE11/11-49/11-49-3.HTM

A person is guilty of fraudulent use of a credit card if he:

- With intent to defraud the issuer or a person or organization providing money, goods, services, or anything else of value or any other person, 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 or she knows is forged, expired, or revoked.
- Obtains money, goods, services, or anything else of value by representing, without the consent of the cardholder, that he or she is the holder of a specified card or by representing that he or she is the holder of a card and the card has not in fact been issued.

If the value of all moneys, goods, services, and other things of value obtained does not exceed $100 in any six month period, it is punishable by up to one year in prison and/or a fine up to $1000. If the value exceeds $100 in any six-month period, it is punishable by up to three years in prison and/or a fine up to $3000.

Statute: §11-49-4: http://www.rilin.state.ri.us/Statutes/TITLE11/11-49/11-49-4.HTM

It is unlawful to make or cause 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 or her identity or that of any other person, firm, or corporation or his or her financial condition or that of any other person, firm, or corporation, for the purpose of procuring the issuance of a credit card. Violations are punishable by up to one year in jail and/or a fine up to $1000.
Statute: §11-49-2: http://www.rilin.state.ri.us/Statutes/TITLE11/11-49/11-49-2.HTM

Social Security Numbers: State law places limits on the use and dissemination of Social Security numbers (SSNs). The law will not permit a person, business, or state or local agency to:

- Intentionally communicate or otherwise make available to the general public an individual's Social Security number;
- Print an individual's SSN on any card required for the individual to access products or services provided by the person or entity;
- Require an individual to transmit his or her SSN over the Internet, unless the connection is secure or the Social Security number is encrypted;
- Require an individual to use his or her SSN to access an Internet Website, unless a password or unique personal identification number or other authentication device is also required; and
- Print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires the SSN to be on the document to be mailed.

Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment purpose; to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the SSN. A SSN that is permitted to be mailed may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened. The provisions do not apply to documents that are recorded or required to be open to the public. Violations are punishable by a civil fine of up to $3,000. A person who knowingly violates the provisions is guilty of a misdemeanor, punishable by up to thirty days in prison and/or a fine up to $5,000.
Statute: §6-48-8: http://www.rilin.state.ri.us/Statutes/TITLE6/6-48/6-48-8.HTM

Spyware: It is unlawful for a person who is not an owner or operator to transmit computer software to the owner or operator's computer with actual knowledge or with conscious avoidance of actual knowledge and to use the software to do any of the following:

- Modify, through intentionally deceptive means, settings that control any of the following: a computer's home page, the default search engine, or the owner's list of bookmarks.
- Collect, through intentionally deceptive means, personally identifiable information, either through the use of a keystroke-logging function that records all keystrokes made by an owner or operator and transfers that information from the computer to another person or in a manner that correlates such information with data respecting all or substantially all of the websites visited by an owner or operator, other than websites operated by the person collecting such information; or by extracting information from the owner or operator's hard drive.
- Prevent, through intentionally deceptive means, an owner or operator's reasonable efforts to block the installation or execution of, or to disable, computer software by causing the

software that the owner or operator has properly removed or disabled automatically to reinstall or reactivate on the computer;
- Intentionally misrepresent that the computer software will be uninstalled or disabled by an owner or operator's action;
- Through intentionally deceptive means, remove, disable, or render inoperative security, antispyware, or antivirus computer software installed on the computer;
- Modify any of the settings related to the computer's access to, or use of, the Internet, including settings that protect information about the owner or operator in order to steal the owner or operator's personally identifiable information; and security settings.

Statute: §11-52.2: http://www.rilin.state.ri.us/Statutes/TITLE11/11-52.2/INDEX.HTM

Victim Assistance:

Security Breach: State law requires any state agency or business that owns, maintains, or licenses computerized data that includes personal information to disclose any breach of the security of the system that poses a significant risk of identity theft to any Rhode Island resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A security breach occurs upon "unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency or person."

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. Notification of a breach is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, a determination is made that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired.

Personal information is defined as an 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 and data elements are not encrypted: Social Security number; driver's license number or Rhode Island Identification Card number; or an 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 or e-mail. If the cost of providing regular notice would exceed $25,000, the amount of people to be notified exceeds 50,000, or the business 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, conspicuous posting on the business's or agency's web site, and notification to major statewide media.

Statute: §11-49.2: http://www.rilin.state.ri.us/Statutes/TITLE11/11-49.2/INDEX.HTM

Credit Freeze: All Rhode Island 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. 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: §6-48-1 through 7: http://www.rilin.state.ri.us/Statutes/TITLE6/6-48/INDEX.HTM

How to Place a Security Freeze in Rhode Island:
http://www.consumersunion.org/pdf/security/securityRI.pdf

State Resources:
State Police, "Identity Theft" (http://www.risp.ri.gov/idtheft/)
The document directs victims to: "*Report the crime to their state or local police department. A request should be made for license and registration checks in order to identify possible unlawful activity. Victims should provide all information which may reveal the manner in which the identity was unlawfully obtained and describe any known fraudulent activity*."

Legislation:

2006:
Passage of **HB 7148** will allow Rhode Island 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.

In addition, the bill increases protections of Social Security numbers (SSNs). Businesses and state and local government agencies are prohibited from posting SSNs or displaying them in public. The bill also targets the use of Social Security numbers on the Internet. Web sites are banned from requiring SSNs to be used to gain access unless it is in combination with a password and the number is encrypted.

HB 6811 targets the use of spyware, software that surreptitiously monitors a computer user's actions. The bill makes it illegal for anyone to transmit software to another computer without the owner's knowledge or to falsely entice someone to download software. It prohibits an unauthorized person from installing software that would take control of a computer's computer, modify its security settings, collect the user's personal identification information, interfere with its removal, or otherwise deceive the authorized user.

2005:
HB 6191 requires state government agencies and any company that lawfully collects and maintains computerized records containing consumer's personal information to notify affected consumers in the event that personal data is compromised in a security breach.

2003:
H 5871 / S 0663 include the use of financial information with intent to defraud another person or with intent to commit any violation of federal, state or local law as a felony under the impersonation and identity fraud act. It makes it a felony to use financial information, such as account numbers, transactional data concerning any account, codes, passwords, Social Security numbers, tax identification numbers, and driver's license numbers, with the intent to defraud another person or commit any violation of law.