



RIPIRG

11 South Angell Street #337 Providence, RI 02906
(ph) 401.421.6578 (fax) 401.331.5266 www.ripirg.org

Self Defense 101

Four Ways Rhode Island Can Empower Consumers and Protect Them from Identity Fraud and Credit Mistakes

Written By: **Matt Auten, Advocate, Rhode Island Public Interest Research Group¹**

I. Summary of Findings

Identity theft is the taking of another's personal information –such as social security number, name or date of birth—for the purpose of assuming the victim's identity with the intent to commit fraud. Identity theft is among the nation's fastest growing crimes, affecting up to 10 million Americans- and an estimated 12,500 Rhode Islanders- annually.

While Rhode Island has taken some steps to fight identity theft in the past, this report will show that more needs to be done. There are four critical policy steps that Rhode Island should take to immediately fight identity theft.

The four critical steps are:

- Strengthen the state's new security breach notice law.² The law was intended to improve data security and require consumers to be notified when their personal data is compromised, but the current act is inadequate because, among other reasons, it probably would not have covered the recent data breaches of the RI.gov website.
- Enact a strong security freeze law that gives consumers control over their credit reports and prevents identity theft before it happens, as twelve states have already done.
- Establish consumer-driven credit monitoring by giving consumers the right to obtain up to twelve low-cost credit reports each year.
- Limit the availability of Social Security Numbers, which serve as keys that can unlock a consumer's financial identity.

¹ The author would like to thank Edmund Mierzwinski, Consumer Program Director, National Association of State PIRGs, Gail Hillebrand, Senior Attorney, Consumers Union (Publisher of Consumer Reports), Abigail Caplovitz of NJPIRG, Daniel Park and Peter Asen for their editorial assistance.

² RIGL: Section 1, Title 11 [49.2](#)

II. Identity Theft: A Growing Problem in Rhode Island

Advances in electronic data collection and communication have fundamentally altered Rhode Island's financial landscape. The tremendous changes to our banking, credit, insurance, education, and health care systems have undoubtedly benefited consumers, but unfortunately, they have also led to an unprecedented level of collection and storage of personal data.

Interests ranging from credit card companies and credit reporting agencies, to insurance, educational, governmental and healthcare institutions are all collecting and storing our data. The information age has even spawned an information economy: data brokers such as ChoicePoint now exist solely to gather and sell information about consumers.

Many Rhode Islanders were shocked on January 27, 2006 when the Providence Journal reported that, "*Russian hackers claim they accessed credit card information for up to 53,000 transactions... on the RI.gov website.*"³ Violations of this kind are a direct result of the volume of data collection occurring in our society and can be attributed to the carelessness of those storing our personal data.

Unfortunately, the RI.gov incident is not unusual; the amount of data that has been compromised in the past year is staggering. Since the announcement by ChoicePoint of a major data breach on February 15, 2005, over 53 million Americans have been exposed to the risk of ID theft, because some amount of their personal information has been compromised.⁴ In short, consumer's personal data has become readily available and accessible to hackers and identity thieves.⁵

Once identity thieves are able to arm themselves with a consumer's personal information, particularly their Social Security Number, they can gain access to their identity and credit reports, allowing them to commit a wide range of identity crimes including: opening fraudulent credit card, cell phone, insurance, employment and utility accounts.

Identity theft has been called one of the nation's fastest growing crimes. In September 2003, the Federal Trade Commission released a survey showing that 27.3 million Americans had been victims of identity theft in the previous five years, including 9.9 million people in the previous year.⁶ According to the survey, identity theft cost businesses and financial institutions nearly \$48 billion, while consumer victims reported \$5 billion in out-of-pocket expenses in 2002.

³ Parker, Paul Edward, Providence Journal, January 17, 2006 Page A1

⁴ <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP> Wednesday, January 25, 2006

⁵ See Appendix A on Page 10

⁶ Federal Trade Commission, *Identity Theft Survey Report*, Sept. 2003, available at: <http://www.ftc.gov/os/2003/09/synovatereport.pdf>.

Extrapolating from data published by the Federal Trade Commission, an estimated 12,500 Rhode Islanders were victimized by identity theft in 2005.⁷

Fortunately, the Rhode Island General Assembly does have the ability to empower consumers and help prevent some cases of identity crimes from happening. This can be done by adopting four comprehensive, yet simple, legislative reforms that are outlined in Section VI of this paper.

III. Credit Bureaus and Credit Reports: A Primer

Credit bureaus collect and compile information about consumers creditworthiness from banks, other creditors and public record sources such as lawsuits, bankruptcy filings, tax liens and legal judgments. The three major credit bureaus—Experian, Equifax, and Trans Union—maintain files on nearly 90 percent of all American adults.

The files that are collected by Experian, Equifax and Trans Union are routinely sold to credit grantors, landlords, employers, insurance companies and many others interested in the credit record of a consumer. These transactions often occur – legally - without a consumer's knowledge or permission. This is the loophole that identity thieves rely on to gain access to consumers' personal information. As long as a business has a permissible purpose to review a credit report, credit bureaus don't ask who the applicant is; they merely match a credit report to the Social Security Number provided and issue the report.

Several studies since the early 1990s have documented sloppy credit bureau practices that lead to mistakes on credit reports—for which consumers pay the price. The most recent study of credit reports, researched by the State PIRGs, found that twenty-five percent of surveyed reports contained serious errors such as false delinquencies, or accounts that did not belong to the consumer.⁸ Other reports have also found similar problems with credit reports.⁹

⁷ Based on calculations with data from <http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf> p. 60 Monday, January 30, 2006, and data from http://www.consumer.gov/idtheft/pdf/synovate_report.pdf p.51, Monday, January 30, 2006

⁸ State PIRGs, *Mistakes Do Happen*, June 2004, available at: <http://uspirg.org/reports/MistakesDoHappen2004.pdf>

⁹ See, Consumers Union, *What Are They Saying About Me? The Results of a Review of 161 Credit Reports from the Three Major Credit Bureaus*, April 29, 1991; Consumer Federation of America and National Credit Reporting Association, *Credit Score Accuracy and Implications for Consumers*, December 2002, available at: http://www.consumerfed.org/121702CFA_NCRA_Credit_Score_Report_Final.pdf; and Robert Avery, Paul Calem, Glenn Canner, and Raphael Bostic, "An Overview of Consumer Data and Credit Reporting," *Federal Reserve Bulletin*, February 2003, available at: <http://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf>. We have reviewed the follow-up study by Avery, Calem and Canner, "Credit Report Accuracy and Access to Credit," *Federal Reserve Bulletin*, Summer 2004, pages 297-322. We disagree with the inferences some have made that this study concludes that the credit bureaus could not do a much better job. In fact, the Federal Reserve study points out that nearly 33% of consumers have missing information in at least one account. The study also makes clear, among other concerns, that some individuals are more affected by errors than others; specifically, individuals with lower scores are more likely to be hurt by mistakes and that false or duplicative collection accounts have a significant negative impact. See, http://www.federalreserve.gov/pubs/bulletin/2004/summer04_credit.pdf

IV. Credit Report Errors Are Serious Business

Credit report errors are serious business for consumers. Consumers with serious errors in their credit reports can be denied credit, home loans, apartment rentals, auto insurance, medical coverage and even the right to open a bank account, or use a debit card. In addition, consumers with serious errors in their reports who eventually succeed in obtaining credit may have to pay higher interest rates because mistakes on their credit reports have falsely placed them in the sub-prime, high-cost lending pool. Other errors that consumers find in their credit reports may be the result of identity theft.

V. The Federal Context

In December 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACT Act).¹⁰ With the FACT Act, Congress significantly amended the Fair Credit Reporting Act (FCRA)¹¹, which provides consumer protections regarding the use, accuracy, and privacy of consumer credit reports. Through passage of the FACT Act in 2003, the financial industry achieved one of its primary goals: the preemption of stronger state credit and privacy laws in many, but importantly, not all, areas.

Since Congress has not done a complete job of protecting citizens from identity fraud and credit bureau mistakes, states like Rhode Island must step in. Thankfully, despite passage of the FACT Act, states are still able to take several important steps to reduce identity theft. This right for states to pass stronger identity theft laws is made very clear in the Congressional history of the FACT Act.¹²

¹⁰ Fair and Accurate Credit Transactions Act (FCRA), Pub. L. No. 108-159, 2003 HR 2622 (2003).

¹¹ Fair Credit Reporting Act, 15 U.S.C.A. § 1681 *et. seq.*

¹² See also the legal memorandum: "After the FACT Act: What the States Still Can Do To Prevent Identity Theft at <http://www.pirg.org/consumer/credit/factmemohillebrand.pdf>

VI. Recommendations

Step 1: Ensure Consumers Know When Their Information May Have Been Stolen or Compromised

In 2005 the General Assembly passed the “Identity Theft Protection Act of 2005.” The intent of this law was to ensure Rhode Islanders that businesses that own or license personal information would be required to provide reasonable security for that information.

The law also required that consumers be notified anytime there is:

*“...a breach of the security of the system which poses a significant risk of identity theft following discovery or notification of the breach in the security of the data to any resident of Rhode Island whose **unencrypted personal information** was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, to acquire said information...”¹³*

While this law was a good first step towards ensuring data security, giving Rhode Island consumers the right to know when their personal information may have been stolen and specifying their ability to recover damages, it probably would not have ensured that Rhode Islanders the right to notification after the RI.gov website was hacked, because that data was originally encrypted.

This is a major problem, because as the *Providence Journal* reported, the original encryption of the RI.gov data did not stop the RI.gov hackers from making use of the information on the website.¹⁴ Most likely this was because the encryption was either inadequate, or because the encryption key may have been available to the thieves. Regardless, the RI.gov incident is clear evidence that the law passed last year must be revisited.

The Rhode Island General Assembly should pass legislation this year to ensure that Rhode Islanders know when their personal information has been breached, regardless of whether that information came from a site that was originally encrypted or not. Encryption should only be a defense if the encryption is so strong that it cannot be cracked. Finally, the law should also explicitly stipulate that the encryption defense should no longer apply if encryption keys are lost with the encrypted data.

¹³ RIGL: Section 1, Title 11 **49.2-3**

¹⁴ http://www.projo.com/news/content/projo_20060127_riweb27.1d31d9f7.html Monday, January 30, 2006

Step 2: Preventing New Account Fraud

New account fraud occurs when an identity thief uses a consumer's personal information to open a new account, such as a credit card, in their name. Before opening a new account, potential creditors and other service providers usually require both personal information -like a name, address and social security number - and access to one or more credit reports from the credit reporting bureaus.

New account fraud thus relies on both on the ability of identity thieves to harvest easily available personal information, and the willingness of credit reporting agencies to sell a credit report to third party businesses, as long as the Social Security Number and name match.

In an ideal world, personal information – including Social Security Numbers – wouldn't be easy for thieves to obtain. However, given the realities of the information age, consumers need to be able to protect themselves from new account fraud even if their social security numbers have been compromised. Security freezes afford consumers that protection.

Security freezes give consumers the ability to control access to their credit reports by protecting them with a personal pass-code, akin to an ATM PIN number. Security freezes work to prevent new account fraud, because most potential creditors can't issue credit without first reviewing one, or more, of a consumer's credit reports.

If a consumer can control access to their credit reports, then most identity thieves won't be able to get new credit in their name, regardless of how much of a consumer's personal information they have stolen or acquired. Therefore, security freezes are a great tool for consumers to stop fraudulent credit seekers in their tracks

The Rhode Island General Assembly should empower consumers to stop new account fraud this year, by passing legislation giving Rhode Islanders the ability to voluntarily place a security freeze on their credit reports free of charge.

California, Colorado, Connecticut, Illinois, Louisiana, Maine, New Jersey, Nevada, North Carolina, Texas, Vermont and Washington have all passed versions of security freeze legislation.¹⁵ In addition, the legislation has been filed in another 15 states.

¹⁵ Cal. Civ. Code § 1785.11.2; Colo.Rev.Stat. § 12-14.3-102, §§ 12-14-106.6 to 106.9; 2005 Conn. Pub. Acts 148; 815 ILCS 505/2MM; La. Rev. Stat. Ann § 9.3571(H) to (Y); 2005 Me. Laws 243; NJ Pub. Law 2005, c. 226; 2005 Nev. Stat. 391; 2005 N.C. Sess. Laws 243; Tex. Bus. & Com. Code Ann. § 20.031 to 20.039; 9 Vt. Stat. Ann. § 2480a to 2480j; 2005 Wash. Laws 342.

Step 3: Increasing Access to Credit Reports

The prevalence of identity theft and credit report errors requires consumers to be vigilant about monitoring their credit reports to detect fraud and inaccuracies. Several studies have documented sloppy credit bureau practices that lead to mistakes on credit reports. Credit report errors can be very serious business for consumers, as detailed in Section II of this report.

Federal law currently allows consumers one annual free credit report on request from each of the national credit bureaus¹⁶. While this is an important consumer protection, checking a credit report once a year does not allow consumers to adequately detect mistakes or cases of identity fraud. The major credit reporting agencies are currently taking advantage of consumers' need to monitor their reports by marketing expensive credit monitoring services to consumers.

This marketing is inappropriate and may be deceptive, since credit reporting agencies' own lax procedures cause or facilitate inaccuracies and fraud; and they then compound the problem by selling these additional services to facilitate the discovery of these errors.¹⁷

To make matter worse, credit reporting agencies have ignored their statutory duty to take reasonable steps to ensure the maximum possible accuracy of consumers' credit reports. As such, the proper public policy would be to require credit reporting agencies to provide consumers with more regular, affordable access to their reports, so that mistakes may be identified and corrected and identity theft could be spotted more quickly.

While the federal Fair Credit Reporting Act does preempt states from requiring more free access to consumer credit reports than the one annual report provided for by federal law, states do retain the right to regulate the price of non-free credit reports.

Rhode Island should pass legislation this year to allow consumers monthly access to their credit reports for a fee of up to two dollars per report, for up to twelve reports a year. This will empower consumers to monitor their own credit reports, while helping consumers to reduce credit report errors and catch instances of new account fraud.

¹⁶ Suspected victims of fraud, consumers who have recently been denied credit, the unemployed looking for work and the indigent can also obtain a free credit report under federal law.

¹⁷ See, e.g., "Marketer of "Free Credit Reports" Settles FTC Charges: "Free" Reports Tied to Purchase of Other Products; Company to Provide Refunds to Consumers," 16 August 2005, where Experian was ordered by the FTC to pay a \$950,000 fine plus consumer restitution for its marketing of its credit monitoring services, available at <http://www.ftc.gov/opa/2005/08/consumerinfo.htm> (last visited 6 November 2005).

Step 4: Social Security Number Protection

Social security numbers are widely used as an identifying marker for consumers, making it relatively easy for thieves to use stolen or purchased social security numbers to assume innocent consumers identities, and gain access to financial accounts and other sensitive information.

Consequently, the use of consumers' social security numbers for transactions, credit applications, or on drivers' licenses and other identification should be limited, or prohibited. Social Security numbers are the key to a consumer's financial identity. No person should be required or coerced into providing a social security number, unless it is essential to the transaction and no other identifying information will suffice.

Similarly, universities, health insurers and the military should not use social security numbers as identifiers in information systems or on identification cards. The sale or public display of social security numbers should also be restricted. Limiting the collection and approved uses of the social security numbers will help to reduce new cases of identity theft.

Several states, including Arizona, California, Connecticut, Illinois, Indiana, New Jersey, North Carolina, and Texas have enacted legislation regarding the private sector use of social security numbers. Rhode Island has taken some steps in the right direction, but the state should pass legislation this year to finish the job.

VII. Conclusions

In a time when our personal information has never been more valuable, the protection of that information must remain a high priority. Since the federal government has not fully protected consumers from identity theft, states must step in. Rhode Island has taken some steps forward, but until identity theft becomes a thing of the past, more diligence and leadership are necessary. The Rhode Island General Assembly should act this year to pass legislation that empowers consumers and helps to protect them from identity theft.

Appendix A: Selected Data Breaches

The data breaches listed below are a selected list of breaches since February 2005. These breaches have been reported and posted online by Privacy Rights Clearinghouse, because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers.¹⁸

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint	Bogus accounts established by ID thieves	145,000
Feb. 25, 2005	Bank of America	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures	Hacking	100,000
March 10, 2005	LexisNexis	Passwords compromised	32,000
March 11, 2005	Univ. of CA, Berkeley	Stolen laptop	98,400
March 11, 2005	Boston College	Hacking	120,000
March 20, 2005	Northwestern Univ.	Hacking	21,000
March 28, 2005	Univ. of Chicago Hospital	Dishonest insider	Unknown
April 5, 2005	MCI	Stolen laptop	16,500
April 8, 2005	Eastern National	Hacker	15,000
April 11, 2005	Tufts University	Hacking	106,000
April 12, 2005	LexisNexis	Passwords compromised	Additional 280,000
April 14, 2005	Polo Ralph Lauren/HSBC	Hacking	180,000
April 18, 2005	DSW/ Retail Ventures	Hacking	Additional 1,300,000
April 20, 2005	Ameritrade	Lost backup tape	200,000
April 21, 2005	Carnegie Mellon Univ.	Hacking	19,000
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
May 2, 2005	Time Warner	Lost backup tapes	600,000
May 7, 2005	Dept. of Justice	Stolen laptop	80,000
May 11, 2005	Stanford Univ.	Hacking	9,900
May 20, 2005	Purdue Univ.	Hacking	11,000
May 26, 2005	Duke Univ.	Hacking	5,500

¹⁸ A full list of breaches can be found at: <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP> Friday, March 10, 2006

Self-Defense 101, RIPIRG, April 2006 Page 10

May 28, 2005	Merlin Data Services	Bogus acct. set up	9,000
May 30, 2005	Motorola	Computers stolen	Unknown
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
June 10, 2005	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
June 16, 2005	CardSystems	Hacking	40,000,000
June 22, 2005	Eastman Kodak	Stolen laptop	5,800
June 25, 2005	Univ. of CT (UCONN)	Hacking	72,000
June 29, 2005	Bank of America	Stolen laptop	18,000
July 6, 2005	City National Bank	Lost backup tapes	unknown
July 19, 2005	Univ. of Southern Calif. (USC)	Hacking	270,000 possibly accessed; "dozens"exposed
July 21, 2005	Univ. of Colorado-Boulder	Hacking	42,000
Aug. 22, 2005	Air Force	Hacking	33,300
Aug. 30, 2005	J.P. Morgan, Dallas	Stolen Laptop	Unknown
Sept. 16, 2005	ChoicePoint	ID thieves accessed; also misuse of IDs & passwords.	9,903
Sept. 17, 2005	North Fork Bank, NY	Stolen laptop (7/24/05) with mortgage data	9,000
Sept. 23, 2005	Bank of America	Stolen laptop with info of Visa Buxx users (debit cards)	Not disclosed
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Nov. 8, 2005	ChoicePoint	Bogus accounts established by ID thieves Total affected now reaches 162,000	17,000 more
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 11, 2005	Scottrade Troy Group	Hacking	Unknown
Nov. 19, 2005	Boeing	Stolen laptop with HR data incl. SSNs and bank account info.	161,000
Dec. 1, 2005	Firsttrust Bank	Stolen laptop	100,000
Dec. 2, 2005	Cornell Univ.	Hacking. Names, addresses, SSNs, bank names and acct. numbers.	900
Dec. 12, 2005	Sam's Club/Wal-Mart	Unknown. Exposed credit card data at gas stations.	Unknown
Dec. 16, 2005	La Salle Bank, ABN AMRO Mortgage Group	Backup tape with residential mortgage customers lost in	[2,000,000] Not included in

		shipment by DHL, containing SSNs and account information. Eventually DHL found the lost tape.	total below
Dec. 20, 2005	Guidance Software, Inc.	Hacking. Customer credit card numbers	3,800
Dec. 22, 2005	Ford Motor Co.	Stolen computer. Names and SSNs of current and former employees.	70,000
Dec. 28, 2005	Marriot International	Lost backup tape. SSNs, credit card data of time-share owners	206,000
Jan. 2, 2006	H&R Block	SSNs exposed in 40-digit number string on mailing label	Unknown
Jan. 9, 2006	Atlantis Hotel - Kerzner Int'l	Dishonest insider or hacking. Names, addresses, credit card details, Social Security numbers, driver's licence numbers and/or bank account data.	55,000
Jan. 12, 2006	People's Bank	Lost computer tape containing names, addresses, Social Security numbers, and checking account numbers.	90,000
Jan. 17, 2006	City of San Diego, Water & Sewer Dept.	Dishonest employee accessed customer account files, including SSNs, and committed identity theft on some individuals.	Unknown
Jan 27, 2006	State of RI web site	Hackers obtained credit card information in conjunction with names and address	4,117
Jan 21, 2006	Boston Globe and The Worcester Telegram & Gazette	Inadvertently exposed. Credit and debit card information along with routing information for personal checks printed on recycled paper used in wrapping newspaper bundles for distribution.	240,000 potentially exposed

Appendix B:

For a discussion of what ability states have to tackle identity theft and fraud see: *After the FACT ACT: What States Can Still Do to Prevent Identity Theft*

Gail Hillebrand, Senior Attorney, Consumers Union is available at:

<http://www.consumersunion.org/creditmatters/creditmattersupdates/001640.html>