



Illinois Public Interest Research Group

407 S. Dearborn, Ste. 701 Chicago, IL 60605

WWW.ILLINOISPIRG.ORG

BRIAN@ILLINOISPIRG.ORG

Protecting Consumers from Identity Theft

Real Policy Solutions to Protect Consumers from Sloppy Bank and Other Industry Practices

For More Information Contact: Brian Imus 312-364-0096 x210

IDENTITY THEFT AND A PROPER RESPONSE

Identity theft represents one of the most perilous hidden dangers to an individual's financial well being. The taking of another's personal information – social security number, name or date of birth—for the purpose of assuming the victim's identity to commit fraud, is the fastest growing white collar crime in the country.

Information has become big business. Whether buying the week's groceries, calling family across the state, ordering an airplane ticket or going to the doctor, companies are collecting information about their customers. These records can include not only the consumer's address and social security number, but also their account balances, shopping habits and much more. Yet consumers have no control over what is done with that information.

In 2005 at least 53 million consumers have been placed at risk of identity theft or fraud due to sloppy practices at banks, department stores, data brokers, and even universities and state agencies.

Roughly 10 million Americans a year become victims of identity theft according to the FTC. Though figures vary, over 11,000 Illinoisans reported that they had become victims this past year. With an estimated 81% of victims not reporting the crime, a more realistic figure would be over 46,000 Illinois victims, each year.

The federal government has shown no leadership in protecting consumers from identity theft. It is up to the states to give consumers the protection they need from the sloppy practices of companies that hold customers financial DNA. This paper outlines the problems of identity theft, what other states have done about those problems and what Illinois can do to become the national leader in identity protection.

EASILY AVAILABLE INFORMATION LEADS TO IDENTITY THEFT

Despite claims by the banking and data broker industries, identity theft doesn't just happen at home (relatives, former roommates, acquaintances, etc). In fact, when you add in garbage bins, peeping at the ATM, stolen mail or wallets, the total represents only about 60% of the sources of consumer information for identity thieves.¹ Further, the Federal Trade Commission (FTC) has found that only about half of all victims ever find out how their information was acquired.

Even someone who zealously protects his or her personal financial information has no way to protect what may be the largest pool of information that data criminals use; thefts from the companies and institutions that compile, collect and resell our valuable personal information. Since January 2005, when a California law took effect which required public disclosure of any security breach into information databases, data brokers and other companies have demonstrated a record of overwhelming failure to adequately protect our information.

At the same time, the credit bureaus have proven to be an inadequate gatekeeper to our credit histories, making identity theft an easy crime.

Credit bureaus collect and compile information about consumer creditworthiness from banks and other creditors and from 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. Those files are routinely sold to credit grantors, landlords, employers, insurance companies, and many others interested in the credit record of a consumer, often without the consumer's knowledge or permission. 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.²

Consumers with serious errors in their credit reports can be denied credit, home loans, apartment rentals, auto insurance, or even medical coverage and the right to open a bank account or use a debit card. Consumers with serious errors in their reports who do obtain credit or a loan may have to pay higher interest rates because the mistakes falsely place them in the sub-prime, high-cost lending pool.

Some of the errors in credit reports are the result of identity theft. Despite the industry's dependence on personal information, shoddy protective practices mean that some consumers undeservedly pay a higher price for being victims.³ Though each person faces different obstacles, a victim of ID theft can expect to spend over \$1,000 and spend at least 60 hours untangling their finances from identity theft.

¹ Javelin Strategy & Research and the Better Business Bureau, 2005 Identity Fraud Survey Report, Jan 2005. <<http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html> > (17 Jan 2006).

² Ed Mierzwinski, All About Credit Reports, Credit Scores and Credit Bureaus 3 Dec 2005, <<http://www.pirg.org/consumer/credit/reports.htm> > (16 Jan 2006)

³ For more on this see U.S. PIRG, Mistakes Do Happen: A Look at Errors in Consumer Credit Reports, 2004. <<http://uspirg.org/uspirg.asp?id2=13649&id3=USPIRG&>> (16 Jan 2006)

When the thief applies for credit, or a cell phone, it's the creditor that requests a credit report. Since the creditor is a trusted partner to the credit bureaus, the report is issued even when everything doesn't match. As long as there is a valid Social Security Number in the inquiry, a report can generally be issued. The thief doesn't see the report; the thief simply gets the card, or the phone.

Industry-driven products, such as credit monitoring, cannot stop identity theft. If a customer discovers an inquiry has been made on their report, it's already too late to stop identity theft. The real solution is to prevent, or freeze the report, from being issued in the first place.

There is no excuse for placing the credit-ability of millions of Americans at risk because the system meant to protect their vital financial information is fundamentally broken. And while it is difficult for individuals to completely protect their name, birth date and social security number from being stolen, there are policy initiatives that can better protect consumer's credit and identities.

Illinois should take those steps. The record shows that states have long taken the lead in protecting consumers' privacy and ensuring the accuracy of credit reports. In 1992, Vermont was the first state to pass a law providing a free annual credit report on request, followed by Colorado, Georgia, Maine, Maryland, Massachusetts, and New Jersey. California adopted other comprehensive reforms in 1994. California later became the first state to require disclosure of credit scores and protections for identity theft victims. In 2003, Congress finally and begrudgingly followed the states' lead in these areas, adopting the free credit report and access to a credit score as well as enacting some new identity theft reforms.

OUR STATE'S PROGRESS

Illinois has taken some major steps forward to protect consumers. Over the past three years Illinois's legislature prohibited the printing of credit card numbers on customer receipts (Public Act 93-0231 (93rd G.A. HB 259), protected social security numbers from being needlessly overused (Public Act 93-0739 (93rd G.A. HB 4712)), required companies to announce any security breaches to their information databases (Public Act 94-0036 (HB 1633)). As well, a law was passed that allows victims of identity theft to place a security freeze on their credit report (Public Act 94-0074 (HB 1058)). While these are good steps towards curtailing identity theft and fraud, more must be done in Illinois to prevent weak industry protective measures from disrupting our lives.

SOLUTIONS

In Illinois there are measures we must take to stop identity theft and ease the burden on those who have been victims.

1) EXTEND SECURITY FREEZE TO ALL ILLINOISANS

All consumers should have the right to place a security freeze on a credit report. Only the security freeze prevents future unwanted extensions of credit. Only the security freeze allows individual consumers to take control of their own financial DNA. Only the security freeze will keep thieves with access to your social security number from getting credit on your name.

In 2005 the Illinois Legislature passed Public Act 94-0074 (HB 1058) which protects some citizens from identity theft. The law allows victims of identity theft to place a security freeze, a password protection, on their credit report. But why should this critical right only accrue to those who've already faced the indignity of identity theft? Why shouldn't it be used to prevent identity theft in the first place?

Illinois should join California⁴, Colorado⁵, Connecticut⁶, Louisiana⁷, Maine⁸, Nevada⁹, New Jersey¹⁰ and North Carolina¹¹ in allowing ALL consumers to place a security freeze on their credit reports.¹² A credit report is the key that unlocks the door to obtaining a loan, getting a credit card or obtaining a cell phone contract. We shouldn't give that key to identity thieves. We can starve credit thieves by barring access and protecting our credit reports.

2) ADEQUATE DESTRUCTION OF PERSONAL RECORDS

As long as valuable information is collected, unscrupulous employees, hackers and other thieves will attempt to steal it. Unfortunately, many companies and institutions needlessly endanger consumers by not taking enough care when disposing of names, social security numbers and credit card info of former customers, employees, students or members. To prevent sensitive personal information from falling into the hands of identity thieves, Illinois should require businesses to properly dispose of records that contain information that could be used to impersonate an individual. In April 2005, 180,000 customers' information was stolen because Polo Ralph Lauren Corporation's point-of-sale system (through HSBC Holdings PLC) stored credit card data instead of purging it immediately after transactions were completed.

⁴ California Civil Code Section 1785.10-1785.19.5

⁵ Colorado Senate Bill 05-137

⁶ Connecticut Public Act No. 05-148

⁷ Louisiana Act No. 766/ House Bill No. 623

⁸ Maine LD 581

⁹ Nevada Senate Bill No. 80

¹⁰ New Jersey A4001

¹¹ North Carolina Senate Bill 1048 / S.L. 2005-414

¹² To review all these laws plus laws that are being considered in other states visit <http://www.pirg.org/consumer/credit/statelaws.htm>

Because Polo Ralph Lauren Corp was not more attentive to its customer's safety their customers were at risk and potentially became identity theft victims.

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) was intended primarily to help consumers fight the growing crime of identity theft. Section 216 of FACTA and its implementing regulations require proper disposal only of that consumer information which is derived from credit reports. There is no federal law generally requiring proper disposal of all business records containing sensitive personal information of individuals.

Several states, including California, Georgia, Montana, Nevada, New Jersey, North Carolina, Texas, and Wisconsin have enacted legislation similar to this proposal.¹³ California Civil Code §§ 1798.80-82 also known as the "Shredding" Law requires businesses to take reasonable steps to destroy records containing personal information upon disposal of the records by shredding, erasing, or modifying the information to make it unreadable.¹⁴ Our state can continue on a path to be a national leader in consumer protection by requiring businesses and institutions to take reasonable measures to protect against unauthorized access to or use of records containing personal information when disposing of them. In addition, the legislature should extend this requirement to any third-party vendors engaged to dispose of such records. The FACT Act does not preempt states from enacting such provisions; in fact, it explicitly states that the federal disposal provision shall not be construed to alter or affect any disposal requirement imposed under any other law.

3) PROTECTION FOR CREDIT HEADER INFORMATION

The term "credit header" refers to the personal identifying information in a consumer's credit file, including a consumer's name, address, telephone number, social security number, mother's maiden name, and birth date. The unrestricted use and sharing of this information can put consumers at serious risk of identity theft and other harms, including stalking.¹⁵ Unfortunately, with the exception of the consumer's age¹⁶, this kind of sensitive, personal identifying information is not covered by the protections of the federal Fair Credit Reporting Act.¹⁷ As a result, for years the credit bureaus routinely sold this information in bulk to direct marketers, private investigators, and others. Credit bureaus are strictly regulated when they sell credit reports but are not so when they sell your header information.

¹³ Cal. Civil Code Ann. § 1798.80 – 1798.84; Ga. Code Ann. § 10-15-1 – 10-15-2; Mont. Code. Ann. § 31-3-115; Nev.

SB 347; 2005 N.C. ALS 414; NJ Pub. Law 2005. c. 226; Tex. Code. Ann. §48.102; Wis. Stat. § 895.505 (statute applies to financial institutions, medical businesses, and tax preparation businesses). Colorado requires both public and private entities to develop policies for the destruction or proper disposal of documents containing personal information. C.R.S. § 6-1-713.

¹⁴ See HB 4229. Working to ensure any state document with personal information is shredded.

¹⁵ A New Hampshire woman, Amy Boyer, was stalked and killed by a man who purchased her social security number from an information broker that had access to the credit header data in Ms. Boyer's credit file. *See*, Kris Axtman, *When Criminals Get Help from the Web*, The Christian Science Monitor (May 9, 2000), available at <http://csmonitor.com/cgi-bin/durableRedirect.pl?durable/2000/05/09/text/p3s1.html>.

¹⁶ Which is associated with derivation of credit scoring models, and so protected as "credit information."

¹⁷ *In re Trans Union Corp.* Docket No. 9255 (FTC, Feb. 10, 2000).

Currently, the federal Gramm-Leach-Bliley Act regulations do provide some protections for these data, but those restrictions are limited.¹⁸ Under the rules, a credit bureau is free to sell consumers' credit header data if the financial institution that gave the bureau the information had first provided its customers with notice and the opportunity to opt out of the sharing.¹⁹ In addition, any personal identifying information that the credit bureau itself collects directly from consumers also can be sold, subject to the bureau's privacy policy. Experian, for example, acquires consumers' personal information when validating consumers' identities for access to online credit reports and monitoring services. Experian's privacy policy suggests that this information is then shared with its affiliates unless the consumer opts-out, and for some of its products, the information is shared with non-affiliated third parties.²⁰

Illinois lawmakers should close these credit header loopholes by limiting the release of this data only to those individuals who would have a permissible purpose to obtain a consumer's credit report under the federal Fair Credit Reporting Act. This is not a law in any state or at the federal level. By passing such a bill, Illinois can trail blaze for the rest of the nation.

4) CONSUMER-DRIVEN CREDIT MONITORING

The prevalence of identity theft and credit report errors requires consumers to be vigilant in monitoring their credit reports to detect fraud and inaccuracies. Federal law allows consumers one free annual credit report from each of the national credit bureaus. While this is an important consumer protection, checking a credit report once a year will not ensure early detection of fraud and mistakes. The major credit reporting agencies take advantage of this by marketing their expensive credit monitoring services to consumers as solutions. This marketing is inappropriate and may be deceptive.²¹ Often the credit reporting agencies' own lax procedures cause or facilitate the inaccuracies and fraud; they then sell services to facilitate the discovery of these errors. In addition, the credit reporting agencies have a statutory duty to take reasonable steps to ensure the maximum possible accuracy of consumers' credit reports. As such, they should be providing consumers with regular, affordable access to their reports so that mistakes may be identified and corrected.

¹⁸ While the Gramm-Leach-Bliley regulations on financial privacy (FTC Final Privacy Rule 16 CFR Part 313 "Privacy Of Consumer Financial Information," 12 May 2000) provide that credit headers can only be sold with "notice and opt-out," those regulations do not affirmatively or completely close off sale of credit headers. See discussion pages 79-82 at <http://www.ftc.gov/os/2000/05/glb000512.pdf> and see *Privacy of Consumer Financial Information*, 16 C.F.R. pt. 313, available at <http://www.ftc.gov/os/2000/05/65fr33645.pdf>.

¹⁹ Several studies have shown that consumers report great difficulty in understanding the terms of these privacy notices and the means for opting out. See, State AG Comments on the GLBA Information Sharing Study, May 3, 2002. <http://www.epic.org/privacy/financial/ag_glb_comments.html>.

²⁰ See, Credit Expert Privacy Policy, available at: https://www.creditexpert.com/CE_Site/Message.aspx?PageTypeID=Privacy, and Scorecard Privacy Policy ("...we reserve the right to disclose all of the nonpublic personal information we collect."), available at: <http://www.experian.com/privacy/scorecard.html>.

²¹ 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> (6 November 2005).

While the federal Fair Credit Reporting Act does preempt states from requiring more free access to consumer credit reports than provided by federal law, states retain the right to regulate the price of non-free credit reports.²² California has passed legislation which allows consumers monthly access to their credit reports for a fee of up to two dollars per report, for up to twelve reports a year. Additional reports cost eight dollars. This allows consumers to engage in their own monthly monitoring. Illinois needs to follow the lead of California and permit Illinoisans to police their own credit reports at a lower cost than credit bureaus charge.

FEDERAL PRE-EMPTION

States have long been the laboratories for innovative public policy, particularly in the realm of environmental and consumer protection. State and local legislatures, smaller and often more nimble than the federal government, can develop and test novel policies to address problems identified by local constituents. If a certain policy works, other states can try it. If the policy fails, the state or local government can quickly modify the policy without having affected residents in all 50 states. Success at the state level then often gives rise to federal policy.

When considering federal policy that could conflict with state policy, Congress and the White House have to choose between establishing federal policy as the minimum protection or "floor," allowing states to enact stronger legislation to supplement that minimum standard, or as the "ceiling," in effect establishing maximum requirements that states cannot supersede. When their corporate campaign contributors are faced with strong consumer and environmental protections at the state level, Congress and the White House often call for "uniform" national regulations that trump state law and set an artificial ceiling.²³ (Of course, they then ignore all of the federalism arguments many of them have historically made.)

Unfortunately industry lobbyists have convinced Congress, the executive branch and the courts to undo most state advances by preempting states with watered down weaker versions of good state laws at a federal level. Federal preemption suppresses the creativity of state problem-solvers and shrinks the marketplace of ideas--leaving us with 'lowest common denominator' solutions across the board. By acting now to enact these laws, our state will become a national advocate for consumer rights and will send a message to Washington not to trump the states.

Industry often makes the argument that compliance with 50 balkanized state laws is burdensome. The notion of 50 different state laws is itself a red herring. The states generally enact a few different laws, then others copy the best. The second red herring in their argument is the burden argument. All a firm needs to do is comply with the strongest state law, nationally, and it has no excess compliance costs.

²² The FACT Act amendments to the federal FCRA grandfather in the existing free report on request laws of Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey and Vermont.

²³ Alison Cassady, [Tying the Hands of States: The Impact of Federal Preemption on State Problem-Solvers](http://uspirg.org/uspirg.asp?id2=13881&id3=USPIRG) National Association of State PIRGs, July 2004.< <http://uspirg.org/uspirg.asp?id2=13881&id3=USPIRG>& > (19 Jan 2006)

And if Congress were to enact a strong enough law to solve the problem, it wouldn't even need to preempt. States are rational actors and wouldn't pass different laws for no reason. But presuming first that Congress may not have all the answers and second that it moves slowly, it makes sense not to preempt, because then the states, if they need to do, can raise the bar some more when new problems arise. The marketplace of public policy ideas is better served with 51 competing sellers, than with only one.

CONCLUSION

In a time when our personal information has never been more valuable, the protection of that information must remain a high priority for the states. Illinois has made excellent strides forward, but until identity theft becomes a thing of the past, diligence and leadership are more necessary now than ever from Illinois lawmakers. Illinois must continue to pass progressive legislation to turn the tide of identity theft and be vocal on the national stage in opposing any federal law that preempts our laws for weaker alternatives. It is in the best interest of lawmakers, consumers and business for the changes above to happen. We must all work together to make Illinois the safest place in the country for the identities of its citizens'.