Author's Draft–Do not cite without permission. To appear in Chander, Radin, Gelman, SECURING PRIVACY IN THE INTERNET AGE (Stanford University Press Forthcoming 2005).

Putting Identity Theft on Ice: Freezing Credit Reports To Prevent Lending to Impostors

Chris Jay Hoofnagle[1]

Introduction: Freezing Credit Reports to Prevent Identity Theft.

Identity theft is a growing problem. It occurs where an individual uses another person's personal information to commit fraud.[2] Most identity theft cases involve the acquisition of the victim's Social Security Number for the purpose of opening new credit accounts known as "tradelines."[3] The impostor may obtain credit cards, wireless phone service, or even establish utilities in a victim's name.[4]

In 2003, in a nationally-representative telephone survey of 1,000 Americans, the Federal Trade Commission (FTC) found that 12% of respondents were a victim of some form of identity theft in the previous five years.[5] The crime affects millions of individuals and imposes billions of dollars of costs on the economy: the FTC found that approximately 9.9 million individuals were victims of identity theft in 2002, that the crime cost businesses $47 billion, and victims incurred $5 billion in losses and 297 million hours in wasted time recovering from the crime.[6]

Prior legislative and regulatory efforts to address identity theft have centered on remedial measures, including the creation of "identity theft affidavits," which assist victims in reporting the crime to creditors and credit reporting agencies.[7] These remedial measures do little to prevent the crime. In fact, even formally criminalizing identity theft has not been effective in curbing its incidence.[8]

Instead of remedial measures, we need deeper changes in the system to prevent impostors from opening tradelines. As Professor Daniel Solove has argued, "many modern privacy problems are

---

[1] Associate Director, Electronic Privacy Information Center (EPIC). The analysis and opinions expressed in this article are those of the author only, and do not necessarily reflect the views of EPIC. I am indebted to Professor Daniel Solove and to Woodrow Neal Harzog, a candidate for L.L.M. at the George Washington Law School, for their insightful comments on this manuscript.

[2] *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, Hearing Before the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information*, Jul. 12, 2000 (testimony of Beth Givens, Director, Privacy Rights Clearinghouse), available at http://www.privacyrights.org/ar/id_theft.htm.

[3] *Id*.

[4] A second, more severe form of the crime known as "criminal identity theft" occurs where an imposter burdens the victim with an arrest record by posing as the victim in altercations with the police. This article does not address criminal identity theft, as that crime poses fundamentally different challenges. *Id*.

[5] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 4-5 (Sept. 2003), at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[6] *Id*. at 7.

[7] FEDERAL TRADE COMMISSION, IDENTITY THEFT AFFIDAVIT, at http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf.

[8] Congress formally criminalized identity theft in 1998, but reports of the crime continue to rise. *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. Law. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998); FEDERAL TRADE COMMISSION, OVERVIEW REPORT AND TIMELINE OF THE IDT PROGRAM, Figure 1, Sept. 2003, available at http://www.ftc.gov/os/2003/09/timelinereport.pdf. In 2004, Congress increased the penalties for using personal information in connection with fraud, terrorism, and numerous federal felonies. Identity Theft Penalty Enhancement Act, Pub. L. 108-275 (Jul. 15, 2004). It is unclear what effect the legislation will have.

systemic in nature. They are the product of information flows.[9] Identity theft is such a problem, as the availability of personal data under current information architectures makes it simple for impostors to obtain the identifiers needed to apply for credit. Solove argues that to address these "problems that are architectural, the solutions should also be architectural."[10] By creating an architecture that secures personal information and by establishing rights for individuals and responsibilities on data collectors, we can reduce the risk of misuse of personal information. Such an architecture encourages more involvement from the individual with respect to data, and often provides incentives for companies and governments to reduce the amount of information they collect.

But even if the general information architecture were revamped to create greater protections for data, identity theft may continue to occur because of lax credit granting practices, such as giving a new credit card to an impostor who has made obvious errors on the credit application. Lax granting practices have continued because the credit reporting system law treats credit issuers, such as retailers and credit card issuers, as trusted insiders. As trusted insiders, credit issuers can easily gain access to reports with or without legal justification. Furthermore, these trusted credit issuers have not adopted sound measures for determining the actual identity of credit applicants. Such protocols allow identity thieves to open new accounts in others' names.

This article proposes a fix to address these weaknesses in the credit granting system. It takes the form of a change in the default state of credit reports from their current "liquid" state to a "frozen" one. That is, our current credit system allows our personal information to flow like water to almost anyone who requests it. Once credit information is released, credit grantors who are operating in an extremely competitive market race to issue new tradelines. This makes it simple for impostors to commit identity theft by obtaining new credit accounts.

Under the proposed system, credit reports would be sealed or "frozen," available only when the individual "thaws" her file, and specifies to whom, when, or in what contexts it should be released. Creditors will not extend tradelines without a credit report, and thus under a frozen credit report system, impostors would have great difficulty in obtaining new accounts. The frozen system would also prevent businesses and others from obtaining credit reports without consumers' full consent, thereby limiting marketing and other impermissible uses of the report.

I begin this article by explaining that identity theft is exacerbated by credit grantors who irresponsibly issue tradelines to impostors. Three factors in irresponsible lending are explained, and examples are presented of these activities in practice. I then explain the remedial and preventative measures in place, and argue that they are deployed too late or otherwise fail to counter the forces that drive irresponsible lending activity. I then explain the shift to a frozen system in greater detail, and argue that building in simple barriers to obtaining a credit report

[9] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L. J. 1227, 1232 (2003).

[10] *Id*. at 1241. One generally accepted architectural framework is "Fair Information Practices" as specified by the Organization for Economic Cooperation and Development. *See* Marc Rotenberg, *What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1 (2001); Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 Berk. Tech. L.J. 283 (2003).

will provide a shield for all individuals against most identity thieves. Finally, the last section responds to anticipated objections to a shift to frozen credit.

Clifford J. Dawg: Canine Card Member Since 2004 and Other Examples of Irresponsible Credit Practices.

Clifford J. Dawg is one of the newest holders of a Chase Manhattan Platinum Visa Card. Mr. Dawg enjoys the freedom of a $1,500 credit limit that is accepted worldwide. The problem is that Mr. Dawg is a dog, a four-legged domestic animal that lacks the ability to pay credit card bills or even enter into a credit contract.[11]

In this instance, the owner of the dog had signed up for a free e-mail account in his pet's name and later received a pre-approved offer of credit for "Clifford J. Dawg." The owner found this humorous and responded to the pre-approved offer, listing nine zeros for the dog's Social Security number, the "Pupperoni Factory" as employer, and "Pugsy Malone" as the mother's maiden name. The owner also wrote on the approval: "You are sending an application to a dog! Ha ha ha." The card arrived three weeks later.[12]

Mr. Dawg's owner contacted the issuing bank to cancel the card. According to the owner, the issuing bank explained that Mr. Dawg's name had been acquired from a marketing list.[13] The issuing bank's representative joked that the incident could be used as a commercial with the slogan "Dogs don't chase us, we chase them."[14] Mr. Dawg's Visa card illustrates some of the problems with credit granting. All systems, especially complex ones that are used millions of times, can fail and occasionally produce errors. But Mr. Dawg's case suggests that there is a more systemic problem in the credit application approval process.

The financial services industry might argue that this is an isolated event. Like General "Buck" Turgidson defending the military's unauthorized nuclear attack on Russia in the classic movie Dr. Strangelove, a financial services lawyer might say, "I don't think it's quite fair to condemn a whole program because of a single slip-up."[15] But it is not a single slip up. Credit has been offered and issued to other dogs, including Monty, a Shih-Tzu who was extended a $24,600 credit line.[16] The slip ups also occur with humans. Credit has been granted to children and babies and young teenagers.[17] These events suggest that the credit issuers are lax in their marketing and authentication efforts. It suggests that the applications are processed by a computer, and no human reviews them to prevent fraudulent or improper credit granting.

---

[11] *Dog Gets Carded*, WASH. TIMES (Jan. 30, 2004), available at http://washingtontimes.com/upi-breaking/20040129-031535-6234r.htm; *Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBC SAN DIEGO (Jan. 28, 2004), available at http://www.nbcsandiego.com/money/2800173/detail.html.
[12] *Id*.
[13] *Id*.
[14] *Id*.
[15] DR. STRANGELOVE OR: HOW I LEARNED TO STOP WORRYING AND LOVE THE BOMB (Warner, 1964).
[16] *Identity thieves feed on credit firms' lax practices*, USA TODAY, Sept. 12, 2003, p. 11A; Kevin Hoffman, *Lerner's Legacy: MBNA's customers wouldn't write such flattering obituaries*, CLEVELAND SCENE, Dec. 18, 2002; Scott Barancik, *A Week in Bankruptcy Court*, ST. PETERSBURG TIMES, Mar. 18, 2002, p 8E.
[17] IDENTITY THEFT RESOURCE CENTER, FACT SHEET 120: IDENTITY THEFT AND CHILDREN, available at http://www.idtheftcenter.org/vg120.shtml.

Three factors lead to lax lending practices and inadequate protection of the credit report. First is that under the Fair Credit Reporting Act (FCRA), credit reporting agencies only are required to "maintain reasonable procedures designed" to prevent unauthorized release of consumer information.[18] In practice, this means that credit reporting agencies must take some action to ensure that individuals with access to credit information use it only for permissible purposes enumerated in the Act. The Federal Trade Commission Commentary on the FCRA specifies that this standard can be met in some circumstances with a blanket certification from credit issuers that they will use reports legally.[19]

This certification standard is too weak. It allows a vast network of companies to gain access to credit reports with little oversight. It treats credit issuers and other users of credit reports as trusted insiders, and their use of credit reports and ultimate extension of credit as legitimate. The problem is that insiders can pose a serious risk to security of personal information.[20] For instance, in a high-profile case, criminals relied upon the relationship between Ford Motor Credit Company and credit reporting agency Experian to steal credit reports for identity theft purposes.[21] The criminals used passwords for terminals that gave Ford access to the Experian database. To create this relationship as a trusted user of the credit system, Ford Motor Credit Company would have had to certify that it only obtained and used credit reports for permissible purposes. Despite this certification standard, the criminals were still able to order 30,000 reports using Ford's account before they were caught.[22] Since this fraud occurred over a three-year period, it suggests that a mere certification does not include monitoring or auditing of access to the credit database.

The second factor in lax issuance is that credit grantors do not have adequate standards for verifying the true identity of credit applicants. Credit issuers sometimes open tradelines to individuals who leave obvious errors on the application, such as incorrect dates of birth or fudged Social Security Numbers.[23] Identity theft expert Beth Givens has argued that many incidences of identity theft could be prevented by simply requiring grantors to more carefully review credit applications for obviously incorrect personal information.[24]

---

[18] 15 U.S.C. § 1681e(a).

[19] The Federal Trade Commission is statutorily barred from promulgating regulations on the FCRA. 15 U.S.C. § 1681s(a)(4). The agency issues a non-binding commentary on the Act. Credit, Trade Practices, 16 CFR § 600, 607 (1995).

[20] Brooke A. Masters & Caroline E. Mayer, *Identity Theft More Often an Inside Job, Old Precautions Less Likely to Avert Costly Crime, Experts Say*, WASH. POST, Dec. 3, 2002, p. A1.

[21] Benjamin Weiser, *Identity Ring Said to Victimize 30,000*, N.Y. TIMES, Nov. 26, 2002, p A1.

[22] *Id.*

[23] *See Nelski v. Pelland*, 2004 U.S. App. LEXIS 663 (6th Cir. 2004) (phone company issued credit to impostor using victim's name but slightly different Social Security Number); *United States v. Peyton*, 353 F.3d 1080 (9th Cir. 2003) (impostors obtained six American Express cards using correct name and Social Security Number but directed all six to be sent to the impostors' home); *Aylward v. Fleet Bank*, 122 F.3d 616 (8th Cir. 1997) (bank issued two credit cards based on matching name and Social Security Number but incorrect address); *Vazquez-Garcia v. Trans Union De P.R.*, Inc., 222 F. Supp. 2d 150 (D.P.R. 2002) (impostor successfully obtained credit with matching Social Security Number but incorrect date of birth and address); *Dimezza v. First USA Bank, Inc.*, 103 F. Supp. 2d 1296 (D.N.M. 2000) (impostor obtained credit with Social Security Number match but incorrect address)..

[24] *Legislative Hearing on H.R. 2622, The Fair and Accurate Credit Transactions Act of 2003, Before the Committee on Financial Services*, Jul. 9, 2003 (testimony of Chris Jay Hoofnagle, Deputy Counsel, Electronic Privacy Information Center).

TRW Inc. v. Andrews illustrates the problems with poor standards for customer identification.[25] In that case, Adelaide Andrews visited a doctor's office in Santa Monica, California, and completed a new patient's information form that requested her name, birth date, and Social Security Number.[26] The doctor's receptionist, an unrelated woman named Andrea Andrews, copied the information and used Adelaide's Social Security Number and her own name to apply for credit in Las Vegas, Nevada. On four occasions, Trans Union released Adelaide's credit report because the Social Security Number, last name, and first initial matched. Once Trans Union released the credit reports, it made it possible for creditors to issue new tradelines. Three of the four creditors that obtained a credit report issued tradelines to the impostor based on Adelaide's file, despite the fact that the first name, birth date, and address did not match.[27]

California has attempted to address the customer identification problem by requiring certain credit grantors to comply with heightened authentication procedures. California Civil Code § 1785.14 requires credit grantors to actually match identifying information on the credit application to the report held at the credit reporting agency. Credit cannot be granted unless three identifiers from the application match those on file at the credit bureau. However, this protection only applies when an individual applies for credit at a retailer.[28] Thus, Internet, telephone, and mail credit granting is not covered. Furthermore, the categories of information to be matched could probably be found in public records, the white pages, or other readily-available tools. The categories to be matched include "first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number."[29]

The last factor leading to irresponsible credit granting is competition to obtain new customers. Grantors have flooded the market with "pre-screened" credit offers, pre-approved solicitations of credit made to individuals who meet certain criteria. These offers are sent in the mail, giving thieves the opportunity to intercept them and accept credit in the victim's name.[30] Once credit is granted, the thief changes the address on the account in order to obtain the physical card and to prevent the victim from learning of the fraud.[31] The industry sends out billions of these pre-screened offers a year. It 1998, it was reported that 3.4 billion were sent.[32] In 2003, the number increased to an estimated 5 billion.[33]

---

[25] 534 U.S. 19 (2001); Erin Shoudt, *Identity theft: victims "cry out" for reform*, 52 Am. U. L. Rev. 339, 346-7 (2002).
[26] *Id.* at 23-25.
[27] *Id*.
[28] Cal. Civ. Code § 1785.14(a)(1).
[29] *Id*.
[30] *Identity crises -- millions of Americans paying price*, CHI. TRIBUNE, Sept. 11, 2003, p2.
[31] *Id*.
[32] *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, Hearing Before the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information*, Jul. 12, 2000 (testimony of Beth Givens, Director, Privacy Rights Clearinghouse) (*citing* Edmund Sanders, *Charges are flying over credit card pitches*, L.A. TIMES, Jun. 15, 1999, p. D-1), available at http://www.privacyrights.org/ar/id_theft.htm.
[33] Rob Reuteman, *Statistics Sum Up Our Past, Augur Our Future*, ROCKY MOUNTAIN NEWS, Sept. 27, 2003, p 2C; Robert O'Harrow, *Identity Crisis; Meet Michael Berry: political activist, cancer survivor, creditor's dream. Meet Michael Berry: scam artist, killer, the real Michael Berry's worst nightmare*, WASH. POST MAG., Aug. 10, 2003, p W14.

Competition also drives grantors to quickly extend credit. Once a consumer (or impostor) expresses acceptance of a credit offer, issuers approve the transaction with great speed. Experian, one of the "big three" credit reporting agencies, performs in this task in a "magic two seconds."[34] In a scenario published in an Experian white paper on "Customer Data Integration," an individual receives a line of credit in two seconds after only supplying his name and address.[35] Such a quick response heightens the damage to business and victims alike, because thieves will generally make many applications for new credit in hopes that a fraction of them will be granted.

The Existing Protections Against Identity Theft Are Inadequate.

The Fraud Alert: Too Little, Too Late.

A fraud alert is a notice filed at a credit reporting agency by a consumer who suspects that credit fraud may or has occurred. When a credit issuer pulls a report from the agency, the alert is designed to warn a creditor that the applicant may be an impostor.

This protection is only triggered where an individual suspects fraud, where she is aware that she can file the alert, and where she actually does file the alert. But many identity theft victims never experience any indication of fraud until it is too late. A recent study found that 85% of victims discovered the crime in a "negative manner."[36] That is, a denial of credit, employment, or notice from a creditor alerted the victim to a credit problem. The Federal Trade Commission found that when identity fraud involves the creation of a new account in the victim's name, 33% of victims discover the fraud between 1 and 5 months after it occurred.[37] 24% don't discover the fraud for over 6 months.[38]

Once the individual does suspect wrongdoing and triggers an alert, new protections in the Fair and Accurate Credit Transactions Act (FACTA) require that creditors use "reasonable policies and procedures to form a reasonable belief that the user [creditor] knows the identity of the person making the request."[39] This suggests that in the absence of a fraud report, a tradeline can be extended without at least "reasonable policies and procedures" to verify the credit applicant's identity. Such protections should be in place by default, rather than only when fraud is actually expected.

---

[34] EXPERIAN, INC., CUSTOMER DATA INTEGRATION: THE ESSENTIAL LINK FOR CUSTOMER RELATIONSHIP MANAGEMENT WHITE PAPER 15, 2000, available at http://www.experian.com/whitepapers/cdi_white_paper.pdf.
[35] *Id.*
[36] IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 15-6 (Summer 2003), available at http://www.idtheftcenter.org/idaftermath.pdf.
[37] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 20-21 (Sept. 2003), at http://www.ftc.gov/os/2003/09/synovatereport.pdf.
[38] *Id.*
[39] Pub. L. No. 108-159 § 112 (h)(1)(b)(i). FACTA amended the Fair Credit Reporting Act, 15 U.S.C. § 1681.

The fraud alert also allows the consumer to leave a phone number on file at the credit reporting agency. If the phone number is present, the creditor must call it to check whether the credit applicant is an impostor.[40]

Credit Monitoring: Alerting Victims to Fraud That Has Already Occurred.

Credit monitoring is a service that can alert an individual electronically when the credit report is accessed or where some other credit-relevant event occurs. Monitoring does not prevent impostors from acquiring credit in the victim's name. Instead, it allows victims to discover the crime and act quickly to mitigate harm.

Not only is credit monitoring merely reactive to identity theft, it is also expensive. Experian offers "Credit Expert" monitoring for $89.95 a year.[41] Instead of paying that amount, individuals could instead periodically request a credit report every three or four months at the rate set by the Federal Trade Commission, which is currently $9 per report. In 2004, as a result of changes to the FCRA, individuals will became able to request a free report from each of the credit reporting agencies once a year.[42] With that price change is in effect, monitoring service makes sense only for people who have more money than time.

Attempts to Curb Identity Theft Through Negligence Actions Have Failed.

Attorneys have attempted to curb identity theft by bringing negligence actions against sloppy credit grantors. The goal of the cases is to establish a duty of care between the credit issuer and the identity theft victim, and thus give the issuers a stronger incentive to make decisions more responsibly. However, the courts have been reluctant to assign liability to the credit granting companies.

In *Huggins v. Citibank*, the South Carolina Supreme Court rejected the tort of "negligent enablement of imposter fraud."[43] In that case, the plaintiff identity theft victim alleged that banks owe a duty to identity theft victims when they negligently extend credit in their name. The defendants argued that no such duty existed because the victim was not actually a customer of the bank. Focusing on the requirement that an actual relationship exist between victim and tortfeasor before a legal duty arises, the court rejected the proposed cause of action:

> "We are greatly concerned about the rampant growth of identity theft and financial fraud in this country. Moreover, we are certain that some identity theft could be prevented if credit card issuers carefully scrutinized credit card applications. Nevertheless, we decline to recognize a legal duty of care between credit card issuers and those individuals whose identities may be stolen. The

[40] *Id.* at § 112 (h)(1)(b)(ii).
[41] EXPERIAN, INC., CREDIT EXPERT, available at https://www.creditexpert.com/creditexpert/orderpage1.aspx?sc=623000&bcd=productdetail&pkg=DCZ1Y
[42] 15 U.S.C. 1681j.
[43] 355 S.C. 329 (SC 2003).

> relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them.[44]

Other suits have failed as well.[45]

An array of credit-industry groups wrote briefs as amici in followed the *Huggins*. These included the American Bankers Association, American Financial Services Association, America's Community Bankers, Consumer Bankers Association, the Financial Services Roundtable, MasterCard International, Inc., and Visa U.S.A., Inc.[46] These groups must be concerned about liability because periodically, absurd errors in the credit business come to light, such as the situations described above where dogs and babies receive new credit cards. The errors are severe enough that if they were more widely known, policymakers would legislatively create a tort to address negligent credit issuance or amend the FCRA to require heightened consumer authentication standards to prevent identity theft.

Freezing Credit Reports Would Put ID Theft on Ice.

Because it is too easy for impostors to open new accounts in victim's names, and because existing protections are ineffective in preventing identity theft, we need to change the default status of credit report availability. Credit is in a liquid state by default, where credit reports are available to networks of certified credit, resellers of reports, and other businesses. It's simply too easy to obtain a credit report and extend instant credit under the current architecture. For instance, in February 2004, a Massachusetts Attorney General investigation found that for only $320, an investigator was able to purchase a credit report, Social Security number, and bank statement illegally.[47]

In other words, by default, we are continuously open to new credit accounts. This offers great convenience~~it~~ allows one to walk through a shopping mall and, on a whim, buy an expensive item from a complete stranger. This has been referred to as the "miracle of instant credit."[48] But that miracle is accompanied by the miracle of instant identity theft. It allows identity thieves to conveniently apply for credit in victim's names, and rely upon the alacrity of creditors to obtain a new account.

After the change in the default status of credit reports, access to the credit would be frozen by default. Before credit could be granted, the individual would have to "thaw" their credit by contacting a credit reporting agency, and requesting release of the report.

---

[44] *Id.* at 334.
[45] *Garay v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 1331 (E.D.N.Y. 2004); *Smith v. Citibank*, 2001 U.S. Dist. LEXIS 25047, (W.D. Mo. 2001); *Polzer v. TRW, Inc*., 256 A.D.2d 248 (N.Y. App. Div. 1998).
[46] 355 S.C. 329 (SC 2003).
[47] Bruce Mohl, *Firm barred from selling, collecting financial data, Order protects Mass. Residents*, BOSTON GLOBE, Feb. 6, 2004, available at http://www.boston.com/business/personalfinance/articles/2004/02/06/firm_barred_from_selling_collecting_financial_data/.
[48] *How the FTC Is Policing Privacy: Chairman Timothy Muris explains the commission's strategy for trying to protect individuals and how they can help themselves*, BUSINESS WEEK, Jun. 5, 2002, available at http://www.businessweek.com/technology/content/jun2002/tc2002065_9287.htm.

A frozen credit system would require the consumer to establish a business relationship with the credit reporting agency in which an authentication procedure is chosen. For instance, an individual could specify that credit should only be unfrozen when the request to the credit reporting agency is made from a specified work, home, or wireless phone number. Agreed upon passwords could be employed. Or the credit reporting agencies could employ newly-developed "out of wallet" authentication systems. These systems ask individuals questions that a mugger or someone who has just stolen a wallet could not answer. Instead of asking, "what is your Social Security Number," the system would give a series of multiple choice questions such as "do you have an IRA with Fidelity?" or "which of the following companies holds your home mortgage?" These bits of information are in credit reports but aren't readily available to someone who has stolen a victim's wallet.

This system could be highly customized to individuals' comfort level with the risk of identity theft and to their spending behavior. The thaw could be limited for a certain amount of time, say a weekend of shopping, or to certain creditors when the individual knows where she is going to purchase an item.

Finally, spendthrifts and others who simply don't wish to use the thawing process could opt-out of the system, and keep their credit liquid at all times. This could be done by directing the credit reporting agency to release the report to any creditor unless the individual revokes the authorization.

A frozen credit report system would address the three factors in sloppy credit granting explained in section two. Trusted insiders and grantors with poor authentication systems could not obtain a report unless the consumer had specifically thawed the file. Similarly, grantors who send out pre-screened offers and those that grant credit quickly would pose less of a threat in enabling identity theft.

A frozen system also solves a long-standing problem with authorized access to credit reports, the "impermissible pull." This occurs where someone with access to the credit reporting system obtains a report on a consumer without a credit application or existing relationship with the consumer. Impermissible pulls sometimes occur in the context of automobile purchasing.[49] Some automobile salespersons will greet a window-shopping customer and obtain her name. The salesperson then leaves and "pulls" a report using the name only in order to evaluate the seriousness of the shopper or to increase bargaining power. This practice is illegal under the FCRA, but is still common enough that at least one state has addressed it by statute.[50] A frozen system would stop these impermissible pulls unless the consumer had thawed the credit report prior to window shopping.

Objections to and Limitations of a Frozen Credit Report System.

[49] NATIONAL CONSUMER LAW CENTER, FAIR CREDIT REPORTING, (Anthony Rodriguez, Carolyn L. Carter & Willard P. Ogburn, eds., 5th ed., 2003).
[50] La. R.S. § 9:3571.2 (2003).

The financial services industry and retailers are likely to have many objections to a frozen credit system. Consumers may object to some aspects as well. These objections are analyzed below.

Cost.

Objections may be raised that a frozen credit system would add unnecessary costs to credit granting. Credit reporting agencies would have to bear the burden of establishing more formal relationships with all credit-active individuals. Call centers and other infrastructure would have to be improved to accommodate requests for credit freezes and thaws.

This is a valid objection, and certainly, a frozen system would entail costs to retailers, credit reporting agencies, and to financial services institutions. Objections to the shift to frozen credit, however, must be weighed against the costs of the current liquid system. The current system leads to over $50 billion in costs transferred to individuals and businesses annually.[51] Implementation of a frozen system would prevent a large amount of identity theft, and while costly, it would likely be a fraction of the annual cost of the current system.

Viewed from a different perspective, cost may be an argument supporting a shift in credit. A frozen credit system could be less costly in money and time to businesses and individuals than the current liquid system of credit. It would also transfer costs from identity theft victims to those who run and maintain the credit system.

The costs with implementing the proposed system have already been incurred to some extent. California law already allows individuals to exercise a prophylactic freeze on their credit reports. The California law requires individuals to specifically request the freeze rather than keeping in place by default under the system proposed in this article.[52] Once in place, the California freeze prevents almost all releases of the credit report. Consumers can lift the freeze by first contacting the credit reporting agency with identification information, a freeze identity number, and password.[53] Unlike the shift proposed in this article, the California law allows but does not require the credit reporting agency to develop telephone, Internet or other systems to thaw credit.[54] Nevertheless, the presence of the optional freeze system in California suggests that systems are in place that could be scaled to the entire nation.

Inconvenience.

The financial services industry and consumers alike may find a frozen system inconvenient. That is, by changing the default state of credit, it will delay purchasing decisions. Individuals will no longer be able to buy an expensive item without some forethought. A major benefit of the "miracle of instant credit" will be jeopardized, resulting in lost sales.

[51] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 7 (Sept. 2003), at http://www.ftc.gov/os/2003/09/synovatereport.pdf.
[52] Cal. Civ. Code § 1785.11.2(a).
[53] *Id.*
[54] Cal. Civ. Code § 1785.11.2(f).

First, the point of a frozen system is to change the relationships among credit reporting agencies, credit issuers, and consumers. By changing these relationships, costs of identity theft are more properly allocated to those who control the system the credit reporting agencies and creditors. The current system is maximally convenient for credit grantors, but not for consumers. The average consumer may go a year or longer without applying for credit, but the current liquid system is prepared for daily credit granting.

Second, a consumer who wishes to take advantage of discounts associated with opening up a new credit card can still do so. Such consumers could direct the credit reporting agencies to keep their credit in a liquid state permanently, or allow the credit report to be released with weak authentication procedures. This burden can be set to a minimal level so that individuals who, for instance, wish to take advantage of a discount for obtaining a departmental credit card can do so quickly.

Third, a frozen system does not eliminate the benefits of the miracle of instant credit. Rather, the miracle, if it can be termed as such, lies in the ability to of the system to determine an applicant's credit risk. The miracle is the ability of businesses to grant credit reliably to complete strangers. Creditworthiness reporting would be unaffected It is only the process of formally granting credit that will be affected.

Last, the miracle of instant credit has been accompanied by not only the miracle of instant identity theft, but also by the miracle of instant bankruptcy. Consumer bankruptcy is at its highest rate ever at over 1,600,000 households in 2003.[55] Consumer credit debt topped $2 trillion in 2003.[56] Delinquency in credit card payments, accounts that are more than 30 days past due, is at an all-time high as well.[57] Slowing down purchasing decisions may be a good thing. It might lead to more fiscal responsibility and fewer bankruptcies.[58]

Authentication Problems.

A frozen system would require credit reporting agencies to develop authentication systems in order to verify the identity of consumers attempting to release their report. Implementing these systems for over 100,000,000 Americans is difficult. There will be errors in this implementation, resulting in individuals being preventing from accessing credit. Identity thieves will attempt to crack the system too.

This is a serious, but surmountable challenge. The shift in credit is intended to change the relationship between consumers and credit reporting agencies so that individuals are more involved in the dissemination of personal information. This will require credit reporting agencies to establish more formal relationships with consumers. With existing consumers, credit

[55] William Branigin, *U.S. Consumer Debt Grows at Alarming Rate, Debt Burden Will Intensify When Interest Rates Rise*, WASH. POST, Jan 12, 2004, available at http://www.washingtonpost.com/ac2/wp-dyn/A10011-2004Jan12?.
[56] THE FEDERAL RESERVE BOARD, CONSUMER CREDIT, Feb. 6, 2004, available at http://www.federalreserve.gov/releases/g19/Current/.
[57] *Card Delinquents*, CARDTRAK ONLINE, Mar. 28, 2003, available at http://www.cardweb.com/cardtrak/news/2003/march/28a.html.
[58] *See e.g.* Michele Singletary, 7 MONEY MANTRAS FOR A RICHER LIFE : HOW TO LIVE WELL WITH THE MONEY YOU HAVE (2003).

reporting agencies can use the out-of-wallet authentication procedures (questions are posed to the consumer about facts that are unlikely to be in a wallet, such as "what was the amount of your last deposit"). Credit reporting agencies already use this form of heightened authentication when consumers request their own credit reports. But they do not use it when credit grantors request individuals' reports.

With individuals who are new to the credit system, implementing an authentication system is more difficult. New applicants may be introduced into the system by trusted members who are already enrolled, such as the parents of the applicant. New applicants without friends or family members in the system may have to establish a relationship by mail, which may cause some delay.

In the worst case scenario when authentication procedures fail, individuals would have to establish their identity in person with some trusted third party. Already, this infrastructure exists for identification verification in other contexts. For instance, individuals initiate application for a U.S. Passport by visiting a Post Office, presenting identification documents, and completing an application that is eventually processed by the State Department. A similar process could be established using the Post Office, or a trusted private-sector party, such as a money wire service or bank.

Businesses Need Reports Outside the Credit Granting Process.

Businesses normally pull credit reports for "account review" purposes. That is, a mortgagor or credit card company regularly requests credit reports on their customers to keep track of their debt burdens. If their debt burdens increase, the companies may change the terms of a loan, cancel a tradeline, or sometimes grant more credit.

This objection is easily addressed. An exemption would be available to any company with a live credit relationship with the consumer. That would allow businesses to engage in account review, maintenance, and upgrades or credit increases.

Conclusion

With the increasing incidence and severity of identity theft, we need to seek architectural changes to the credit system to protect personal information. Existing proposals have focused on establishing Fair Information Practices, rights and responsibilities in the use of personal information. But this challenge also requires specific changes to the credit reporting system. Freezing credit information from its current liquid state to a frozen one is one such protection. A system that is frozen by default will act as a strong shield against identity thieves who are trying to open new lines of credit in others' names. It will also protect individuals against the thousands of companies with access to the credit system who currently can obtain their credit report with little oversight. Freezing access to credit reports addresses the factors that lead to irresponsible credit granting and identity theft. Some challenges, including cost, inefficiency, and customer authentication would have to be surmounted. Overall, a frozen system places more power over personal information in consumers' control, and is more consistent with privacy norms.