# INTERNALIZING IDENTITY THEFT

Chris Jay Hoofnagle[1]



---

[1] This work was supported by the California Consumer Protection Foundation, Cassandra Malry, Executive Director and by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia, and United Technologies. The protocol was approved by U.C. Berkeley Office for the Protection of Human Subjects CPHS#2007-9-7, the "FACTA Access Study." I am indebted to Professors Deirdre Mulligan, Daniel Solove, Alessandro Acquisti, Jason Schultz, and Jennifer Urban. Jennifer King, Maryanne McCormick, and Aaron Burstein provided valuable advice, as did identity theft experts Evan Hendricks and Mari Frank. Additionally, Madison Ayer and Rick Lunstrum of ID Watchdog were instrumental in the recruitment of data subjects. This article builds upon three earlier works by Chris Jay Hoofnagle focusing upon problems in identity theft: *Putting Identity Theft on Ice: Freezing Credit Reports To Prevent Lending to Impostors*, *in* SECURING PRIVACY IN THE INTERNET AGE 207 (Anupam Chander et al. eds., Stan. Univ. Press 2008), *available at* http://ssrn.com/abstract=650162, *Towards a Market for Bank Safety*, 21 LOY. CONSUMER. L. REV. 155 (2008), *available at* http://www.luc.edu/law/activities/publications/clrdocs/vol21issue2/hoofnagle_bank_safety.pdf, and *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J.L. & TECH. 97 (2007), *available at* http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf.

# ABSTRACT

Why has identity theft remained so prevalent, in light of the development of ever more sophisticated fraud detection tools? Identity theft remains at 2003 levels -- 9.9 million Americans fell victim to the crime in 2009.

One faction explains the identity theft as a problem of a lack of control over personal information. Another argues conversely that identity theft may be caused by a lack of access to personal information by credit grantors. This article presents data from a small sample of identity theft victims to explore a different dimension of the crime, one that suggests alternative interventions.

Drawing upon victim and impostor data now accessible because of updates to the Fair Credit Reporting Act, the data show that identity theft impostors supply obviously erroneous information on applications that is accepted as valid by credit grantors. Thus, the problem does not necessarily lie in control nor in more availability of personal information, but rather in the risk tolerances of credit grantors. An analysis of incentives in credit granting elucidates the problem: identity theft remains so prevalent because it is less costly to tolerate fraud. Adopting more aggressive and expensive anti-fraud measures is extremely costly and jeopardizes customer acquisition efforts.

These business decisions leave individuals and merchants with some of the externalities of identity theft. Victims sometimes spend their own money, and more often, valuable personal time dealing with identity theft externalities. This article concludes by reviewing several approaches to internalizing these costs. Popular approaches specify prescriptive rules to address particularly problematic practices in credit granting, such as using the Social Security number as a password for authentication. These approaches may lead to compliance-oriented approaches and reification. Several commenters have suggested negligence actions as a cure to identity theft, but uncertainty surrounding the duty of care would probably leave many consumers unremunerated. A strict liability regime is suggested because credit grantors are the least cost avoiders in the identity theft context, and because consumers cannot control the credit granting process nor insure against identity theft losses efficiently.

# I. INTRODUCTION

The legal academic literature frames the identity theft problem in two very different ways.

The first is based on the work of Professor Lynn LoPucki who made an early and substantial contribution to the study of identity theft with two articles examining the problem of credit authentication.[2] In his 2003 paper, LoPucki argues that identity theft exploded in incidence in the 1990s because of the inability of credit grantors to authenticate borrowers.[3] This inability was caused by the decline of public life, the gradual removal of contact information from public registers, such as the DMV database, city directories, and the phonebook.[4] Indeed, as Dennis Bailey argues, modern life is akin to a masquerade ball, where we go unrecognized and cannot recognize others.[5] LoPucki argues that this privacy itself -- the deprivation of publicly-available information about our lives -- might have caused the identity theft epidemic and might have also given impostors the ability to masquerade as others undetected:

> It is probably no coincidence that the rise of identity theft coincided with the decline in public identities. That decline began in the 1970s. Credit-based identity theft emerged as a significant problem in the 1980s, hitting epidemic proportions only in the 1990s. The inverse relationship between privacy and public identity -- logically and chronologically -- suggests that privacy is a cause, if not the principle cause, of identity theft.[6]

In the other paradigm, Professor Daniel J. Solove frames identity theft as a problem of a loss of control over personal information. He argues that the traditional model for protecting privacy, one that conceives of harms as discrete events that affect individuals, cannot address new social and technological developments that have created "systemic" changes.[7] For instance, the adoption of the Social Security number (SSN) without protections against misuse has put all Americans at greater risk of identity theft. Solove calls this an "architecture of vulnerability."

> Identity thieves, then, are only one of the culprits in identity theft. The government and private-sector entities bear a significant amount of responsibility, yet this is cloaked in the conception of identity theft as a discrete crime that the victim could have prevented had she exercised more care over her personal data. Identity theft does not merely happen; rather, it is manufactured by a legally constructed architecture.[8]

---

[2] *See* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89 (2001) [hereinafter LoPucki, *Human Identification Theory*]; Lynn LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277 (2003) [hereinafter LoPucki, *Privacy*].
[3] *See* LoPucki, *Privacy*, *supra* note 2, at 1278.
[4] *See id.* at 1277-78.
[5] *See* DENNIS BAILEY, THE OPEN SOCIETY PARADOX: WHY THE 21ST CENTURY CALLS FOR MORE OPENNESS-NOT LESS 26 (2004).
[6] LoPucki, *Privacy*, *supra* note 2, at 1278 (citation omitted).
[7] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1232 (2003).
[8] *Id.* at 1261 (citation omitted).

Solove thus proposes a privacy architecture that reflects the liberal "privacy-control" paradigm identified by Paul Schwartz.[9] Under the Solove approach, individuals would have substantive and procedural rights to learn about credit authentication and to limit dissemination of data. This transparency and control would inhibit impostors from stealing identities.

This article enriches the dimensions explored by LoPucki and Solove through an analysis of a small sample of identity theft cases. Part II of this article explains the Fair and Accurate Credit Transactions Act ("FACTA") Access Study. In this study, impostors' credit applications and other materials were acquired for the purpose of analyzing how businesses authenticated credit applicants. Materials from 16 incidents of identity theft were obtained pertaining to 6 individuals who were victims of financial, medical, and criminal identity theft. Every financial credit application contained some type of incorrect personal information, yet credit grantors chose to extend products and services to the impostor. But the problem is not limited to the financial sector. Other institutions, such as medical care providers and jails, overlooked incorrect personal information when verifying individuals' identities.

In light of these findings, part III of this article adds a new dimension to the LoPucki and Solove approaches, explaining that identity theft cannot be framed as a problem of too much privacy or a lack of privacy-control. I argue that tolerating risk of identity theft and accepting its attendant losses is a rational decision from a business perspective. Of course, all businesses must tolerate some fraud risk. But incentives particular to the credit industry and competition in instant credit markets create an atmosphere that impostors can leverage. The risk of new account fraud is extremely low in light of the volume of new credit accounts that are granted in the United States. Anti-fraud interventions, when scaled to the enormous credit volume exercised by Americans, are often not cost effective. Further, anti-fraud interventions also cause opportunity costs and possible lost sales to competitors that are less circumspect in verifying identities. There is thus some rationality in accepting credit applications of dubious veracity.

Much of the identity theft debate has focused upon improving technical security measures. Some have even suggested adding biometric identifiers to harden payment systems. As Ross Anderson notes, it is common for information security issues to be seen as mere technical problems.[10] But upon deeper analysis, he argues that information security mechanisms "are much more likely to be the desire to grab a monopoly, to charge different prices to different users for essentially the same service, and to dump risk. Often this is perfectly rational."[11] This article follows Anderson's theme: identity theft is a problem of misaligned incentives. This should not be so surprising in light of recent events. The recent economic downturn has elucidated some of the risks taken in mortgage lending, where much more money is at stake in any given transaction. In that

---

[9] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1659 (1999).
[10] Ross Anderson, *Why Information Security is Hard – An Economic Perspective,* CAMBRIDGE COMPUTER LABORATORY 1 (2001), *available at* http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf.
[11] *Id*. at 7.

context, the so called "NINJA" loan arose (No Income, No Job or Assets).[12] It would follow that similar low or no documentation practices would exist in the credit card market.

The consequences of granting credit to impostors is shared with victims and merchants. Victims pay directly and indirectly (through lost time) to remedy new account fraud. Part IV considers approaches to addressing the externalities of the crime. Most public policy interventions seek to address particular risky practices, such as the use of the SSN for authentication purposes. These approaches, including the "Red Flag Rules," create prescriptive rules requiring credit grantors to apply anti-fraud efforts when indications of fraud are present. The benefits and limitations of that approach are discussed, along with approaching identity theft through negligence and strict liability.

I conclude by arguing that strict liability is appropriate, because credit grantors are fully in control of the identity theft problem. Short of freezing one's credit, there is no option enabling consumers to leave the instant credit marketplace. Individuals cannot insure against the risk of identity theft, and exercising care with personal information has no practical effect because credit grantors accept even fabricated data on credit applications. Strict liability would establish a direct financial cost for poor authentication procedures, compensate victims more fairly than the current system, and fuel innovation in new account fraud detection. Additionally, this approach will more directly address the market failure at the heart of the problem: credit grantors that adopt more aggressive anti-fraud efforts will lose sales to less circumspect companies. The current landscape has created a kind of race to the bottom -- where competitors attempt to grant credit as quickly as possible. Proper incentives would introduce some braking where appropriate and create an atmosphere where more careful decisions are rewarded more richly.

# II. THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT ("FACTA") ACCESS STUDY

## A. BACKGROUND AND METHODS

This article concerns "new account fraud," where an impostor opens lines of credit using personal information of another. This is different from "account takeovers," where an impostor commandeers an existing account belonging to the victim. In surveying Americans, the FTC estimated that in 2005, between 1.2 and 2.8 million Americans had been a victim of new account identity theft in the previous year.[13]

Identity theft interventions have primarily focused upon increasing penalties for impostors[14] and on educating consumers. Until recently, credit grantors, the businesses that ultimately decide whether or not to open a new account for an applicant, have largely escaped the regulatory spotlight.

---

[12] Jack Rosenthal, A Sub Subprime Glossary For the Mortgage Scandal, N.Y. TIMES, Aug. 8, 2008, *available at* http://www.nytimes.com/2008/08/17/opinion/17iht-edsafire.1.15360694.html.
[13] FTC, 2006 IDENTITY THEFT SURVEY REPORT (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.
[14] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, (1998).

Good authentication practices among credit grantors are critical to preventing new account identity theft, but the literature points to many examples where impostors used false or erroneous information and were still authenticated as the victim by the business.[15] Credit cards have even been issued to dogs,[16] to children,[17] to fake people,[18] and in response to torn-up credit applications.[19]

The FACTA[20] provides a unique opportunity to examine business authentication practices. That law empowers victims of identity theft to obtain business records associated with the crime from the company that created an account for the impostor in the victim's name. That is, the victim can obtain records, such as the credit application that the impostor submitted to the company and billing statements generated by the fraud. Obtaining these business records serves several functions: it helps victims prove that they did not open the account, it helps victims determine who opened the account, and it causes companies to reevaluate these records when allegations of fraud arise. Prior to the passage of FACTA, this information was only available in the rare circumstance when a victim brought suit against a company for causing or contributing to identity theft.

Advertisements were placed on Craigslist.org offering gift cards for the participation of new account identity theft victims in the San Francisco Bay Area. The protocol called for making FACTA access requests on these victims' behalf to obtain the applications for credit made by impostors. Once obtained, the victims would review these applications for accuracy, and the methods of business authentication could be documented.

A large number of individuals responded to the Craigslist.org advertisements, but many challenges were encountered in securing the participation of qualifying victims. Upon learning the process, two responded that the experience of becoming a victim was upsetting, and they feared reopening the subject. Others were victims of credit card fraud, a form of account takeover identity theft that did not qualify for this study. A number called with dubious tales of fraud, in transparent attempts to get a gift card.

---

[15] *See, e.g.,* Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874 (W.D. Tenn. 2007) (permitting negligence claim against defendant bank to continue under Tennessee law where a fraudulent credit application was accepted despite having a false address, phone number, and mother's maiden name).

[16] *See, e.g., Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBC SAN DIEGO, Jan. 28, 2004.

[17] Brigitte Yuille*, Stolen innocence: Child Identity Theft*, Bankrate.com, Jan. 3, 2007, http://www.bankrate.com/nltrack/news/debt/20070103_child_identity_theft_a1.asp.

[18] It is possible to manufacture "synthetic" identities using real SSNs and fake names in order to obtain credit; suggesting that some institutions do not even match SSNs to the applicant's name. Chris Jay Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J. L. & TECH. 97, 101 (2007), *available at* http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf.

[19] *See, e.g.,* Bob Sullivan, Even Torn-up Credit Card Applications Aren't Safe, MSNBC, Mar. 14, 2006, *available at* http://redtape.msnbc.com/2006/03/what_if_a_despe.html; Identity Thieves Feed on Credit Firms' Lax Practices, USA TODAY, Sept. 12, 2003, at 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, at 8E. A specific red flag rule addresses the problem of when "[a]n application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled." Identity Theft Rules, 16 C.F.R. § 681, supp. A to app. A (2009).

[20] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

Having failed to recruit victims through months of general solicitations, an identity theft remediation company, ID Watchdog, [21] was approached. ID Watchdog located five victims of new account theft who had undergone the FACTA access process. ID Watchdog, through an identity theft remediation service, regularly makes FACTA requests to identify impostors and to bolster claims that the victim did not commit the fraud. A sixth victim was recruited independently and performed the FACTA access process.

The materials obtained through the FACTA process were carefully reviewed and victims were interviewed. This process shed some light on the application phase of credit granting, and through this lens, one could see the personal information provided by impostors when obtaining credit in others' names.

Among the victims recruited from ID Watchdog, the requests for FACTA documents were abandoned if a creditor released a victim from the fraudulent obligation. Thus, many of the ID Watchdog victims (X1-X5) had other accounts opened in their name, but the application and materials from these other incidents of identity theft are not available. This obviously presents some bias. It could be that the creditors that released victims from obligations had application materials and other analyses that made it absolutely clear that fraud was present. In such cases, providing the FACTA documentation may expose the credit grantor to suit for negligence in enabling identity fraud.[22] Creditors may also be performing a risk-benefit analysis, where complying with the FACTA access provisions is more costly than simply releasing the victim from the obligation.

There is also bias presented from using the ID Watchdog victims. These are individuals who had identity theft incidents that they sought professional help to remedy. One could conclude that that therefore, the ID Watchdog victims must have experienced more severe forms of fraud. Subjects X1, X4, and X5 did experience significant fraud events, but X2 and X3 had more straightforward cases, consistent with that of X6.

Because of the small sample of victims, and because each victim's experience with fraud was different, an overview of each fraud incident is summarized below.

## 1. THE STUDY PARTICIPANTS

X1 is a victim of multiple incidents of medical identity theft and of criminal identity theft. X1's file contains five intake forms from medical institutions or medical services companies and one from a state jail from 2002-2006. X1's impostor was arrested by police and severed jail time at a state department of corrections using X1's identity; in a separate instance, the impostor's conduct resulted in an open warrant for X1's arrest in a different state. X1's credit report showed 26 fraudulent obligations, and had a credit score of 665 before remedying the fraud. X1 learned of the theft through pre-employment background screening. The impostor had obtained an official out-of-state drivers license with X1's name, SSN and date of birth.

---

[21] ID Watchdog is a for-profit company offering identity theft consultation and monitoring services. *See* ID Watchdog, http://www.idwatchdog.com (last visited March 10, 2010).

[22] Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874 (W.D. Tenn. 2007).

X2 is a victim of financial identity theft. The impostor obtained a $400 loan in X2's name, at 126% APR in 2000. The credit grantor claimed to have verified both addresses provided by the impostor, but X2 never worked or lived at either address. X2's credit report showed four other fraudulent obligations, and had a credit score of 530 before remedying the fraud. All four of these other obligations were for private-label credit cards. X2's impostor had a state-issued identification card in X2's name, and many physical differences separated X2 and the impostor. There is over 100 pound difference in weight, a significant difference in height, different eye color, and the impostor is a different race than X2.

X3 is a victim of financial identity theft. X3 had a credit score of 634 before remedying the fraud, which occurred in 1999.

X4 is a victim of financial, medical, and criminal identity theft. X4's file contains one credit application, an intake form from a medical institution, and an intake form from a state criminal court. X4 is a member of the armed services who lost his wallet in 1999, and did not notice subsequent frauds until 2004, when he received a letter from a collections agency. X4's credit report showed 20 fraudulent obligations, and had a credit score of 662 before remedying the fraud. Other medical institutions were billing X4 over $20,000 for unpaid hospital stays by the impostor. Additionally, the impostor was arrested for committing serious crimes while using X4's identity, accrued traffic tickets, and was in an automobile accident resulting in a civil lawsuit against X4.

X5 is a victim of financial identity theft. X5's file contains four fraudulent successful mortgage applications for well over $1,000,000 in loans, all obtained in 2005. Two other mortgages were successfully acquired by the impostor, but those applications are not available. The impostor's early mortgage loans polluted X5's consumer report; thus while the Consumer Reporting Agencies properly flagged three mortgage loan applications as suspicious, the fourth was not because false information from the earlier loans was incorporated into X5's consumer report. The impostor had a drivers license in X5's name. X5 reports that upon learning that mortgage loans were fraudulent, the holder of the loan would sell the obligation to another company. This resulted in collections agencies pursing X5 three years after the loans were approved. X5 claims that remedying the fraud took over 1,000 hours, but when the impostor was ultimately arrested, X5 could not collect restitution, because X5 did not suffer direct financial loss.

X6 is a victim of financial identity theft. The impostor obtained a private-label credit card in X6's name in 2007. The private-label issuer appears to have only collected a name, signature, and SSN in granting the card. The paper application used does not solicit address, date of birth, or other information. A separate sales authorization slip obtained contains X6's correct SSN.


**Figure 1: In an application used to obtain a private-label credit card in X6's name, the impostor misspelled X6's name (should be Grimmelmann, but appears to be Grimmelan), had a forged signature, and omitted basic metadata. Provided with permission by X6, who has publicly revealed his participation in the study.**

## B. RESULTS

A common pattern of errors emerges from a comparison of the 6 victims. The table below compares the 6 victims, and notes the number of incidences that incorrect information was used by the impostor over the number of applications in the victim's file.

**Table 1: Overview of the Most Common Errors on Applications and Other Impostor Materials**

| Victim Number | Wrong* Address | Wrong Phone | Wrong DOB | Wrong SSN | Wrong DLN | Misspelled Name | Red Flags |
|---|---|---|---|---|---|---|---|
| X1 (6 applications) | 4 | 2 | 1 | | | | |
| X2 (1 application) | 2 | 1 | | | | | |
| X3 (1 application) | 1 | | | | | | |
| X4 (3 applications) | 2 | | | 1 | | | |
| X5 (4 applications) | 3 | | 3 | | 1 | | 3 |
| X6 (1 application) | | | | | | 1 | |

*In this context, "wrong" means an address or phone number never belonging to the victim.

For instance, in X1's case, there were 4 incidents were a wrong address was used, 2 with a wrong phone number, and 1 with an incorrect date of birth. More than one error can occur for each application.

**Table 2: Breakdown of Correct and Incorrect Identifiers by Application Type**

| Victim | Application Type | Correct | Incorrect | Other |
|---|---|---|---|---|
| X1 | Medical | Name, sex | Address, DOB, Employer | SSN left blank |
| | Medical | Name, DOB, Sex | | |
| | Medical | Name, DOB, SSN | Address | Phone, Place of Birth left blank |
| | Medical | Name, DOB, Sex | Address, Phone | |
| | Medical | Name, DOB | Address, Phone | |
| | Jail Intake Form | Name, SSN, Sex, Race | Height and weight somewhat inconsistent with victim | |
| X2 | Short-term loan | Name, SSN, DOB | Work and home addresses, phone. | |
| X3 | Credit Card | Name, DOB | Address | |
| X4 | Credit Card | Name, DOB, SSN | Address, Employer | |
| | Medical | Name | Address | |
| | Court Information Sheet | Name, DOB, Sex, Height | SSN, significant weight difference, Race | |
| X5 | Mortgage | Name, SSN | Drivers license number fake, Address, DOB, Race, Employer, Nearest Relative | 3 CRAs red flag on address discrepancy |
| | Mortgage | Name, SSN | Drivers license number, Address, DOB, Employer | 3 CRAs red flag address discrepancy |
| | Mortgage | Name, SSN | Address, DOB, Employer | 3 CRAs red flag address discrepancy; 1 CRA reports DOB error; appears to be low-documentation loan |
| | Mortgage | Name, SSN | Address, DOB, Employer | Red flags no longer raised because previous mortgages polluted report |
| X6 | Credit Card | SSN | Name misspelled | No addresses or other information collected by application |

These errors cannot be described as minor, transcription errors (e.g., when a single digit is transposed or the like).

### 1. WRONG ADDRESSES

The most common form of error on applications submitted by impostors is an incorrect addresses. Of the 6 fraudulent applications concerning X1, the impostor provided an address never belonging to X1 on 4 of them. X2's single fraudulent application had 2 addresses never belonging to X2; the creditor claimed to have verified both. X3's single fraudulent application had an address never belonging to X3. Of the 3 fraudulent applications concerning X4, 2 had addresses never belonging to X4. Of the 4 fraudulent mortgage applications concerning X5, 3 used addresses never belonging to X5. The fourth mortgage application in X5's name did not belong to her either, but the previous mortgaged polluted her consumer report with false addresses. Thus the fourth mortgage lender may not have detected an address discrepancy at all. X6's application did not solicit an address.

Address Verification Service (AVS) is popularly used in the electronic transaction context to ensure that goods ordered are delivered to the billing address. Merchant acquirers will impose higher liability on businesses that are willing to ship merchandise to a non-billing address, thus, many businesses will not accept unverified addresses. This inexpensive means of verification was either not used or ignored in these cases.

### 2. WRONG PHONE NUMBERS

Of the 6 fraudulent applications concerning X1, the impostor provided a phone number never belonging to X1 on 2 of them. X2's single fraudulent application had a fake phone number. As with addresses, imperfect, but inexpensive phone verification services are commonly available, but apparently not used or ignored in these cases.

### 3. INCORRECT DATES OF BIRTH

Of the 6 fraudulent applications concerning X1, the impostor provided an incorrect DOB on 1 of them. Of the 4 fraudulent mortgage applications concerning X5, the impostor provided an incorrect DOB on 3 of them.

X5's impostor smartly used a DOB in the same month and year of X5's real DOB. Because the issuance of SSNs is often linked to the month in which an individual is born, the impostor's technique successfully fooled a "SSN Validation" tool.[23] Nevertheless, commercially-available tools (most notably, the consumer report) are available to validate SSNs to the applicant's name, but they were either not used or ignored here.

### 4. INCORRECT SOCIAL SECURITY NUMBER

X4's court intake sheet for serious crimes committed by the impostor lists a SSN that does not belong to X4.

---

[23] There is no standard for "validation" of SSNs. Some SSN validation services only match the number to date of birth and do not have the capability of matching to name. This means that impostors can fabricate identities with SSNs that match a certain birth month. *See*, Hoofnagle, *supra* note 18, at 116 (describing "synthetic" identities).

Numerous companies and the federal government itself offer SSN validation tools to check the internal consistency of the number; many also match name to SSN.

### 5. WRONG DRIVERS LICENSE NUMBER

The impostor who acquired mortgages using X5's personal information had a drivers license with X5's name, but a fake drivers license number. This drivers license number had never been issued by the state.

This drivers license number could have been identified as fraudulent using a number of validation tools.

### 6. VICTIM'S NAME MISSPELLED

The application for a private-label card in X6's name was notable for its sloppiness. The impostor scrawled X6's name, misspelling it in two different ways on the application. The credit issuer only required name and signature on the application, but may have requested a SSN orally. The application is undated and does not identify the specific store where the impostor applied. In a receipt accompanying the application, X6's correct SSN is listed, but X6's name is misspelled, but in a different way than the impostor listed it on the application.

It is difficult to visualize this case without illustration, but such a description would breach confidentiality. Imagine instead that an impostor stole the author's identity, must misspelled "Hoofnagle" as "Hoofnle" on the application. Processing the application, the store improves the misspelling to "Hoofnagl." That is the level of error that occurred here.

### 7. RED FLAGS RAISED

Sections 114 and 315 of the FACTA[24] required federal agencies to promulgate regulations "requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing . . . [identity theft guidelines] . . . to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers . . . ."[25] A "red flag" is a "pattern, practice, or specific activity that indicates the possible existence of identity theft."[26] In a supplement to the appendix to the Rule, the agencies identify 26 red flags. They include, warnings that the creditor grantor receives from a consumer reporting agency, the presence of suspicious documents, the provision of suspicious personal identifying information, suspicious account activity, and notice from individuals that fraud is afoot.[27]

Once detected, the rules require "appropriate responses" to the red flags "commensurate with the degree of risk posed."[28] Suggested responses include account

---

[24] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).
[25] 15 U.S.C. § 1681m(e)(1)(B) (2009).
[26] Identity Theft Rules, 16 C.F.R. § 681.1(b)(9) (2009).
[27] Identity Theft Rules, 16 C.F.R. § 681, app. A (2009).
[28] *Id.*

monitoring, contacting the customer, or not opening a new account in response to an application.[29]

Automated fraud detection systems at the consumer reporting agencies indicated that fraud could be present in 3 of the 4 mortgage applications in X5's file. One warned, "Substantial difference between address submitted in credit request and addresses in credit file." Two of these red flag warnings indicated that the applicant/impostor's DOB did not match X5's. It is unclear what steps the creditor grantor took to resolve these red flags before extending mortgages to the impostor.

## 8. OTHER OBSERVATIONS

### a) Poor Authentication in the Health Care Setting

Health care providers must balance the conflicting interests of verifying the identities of patients with providing a welcome environment to all who need care. Obviously, in many situations, it may be impossible to obtain reliable identification information from a patient. This in part has contributed to the problem of medical identity theft,[30] which carries with it both the frustrations of financial identity theft and the risk that one's medical file could be polluted with data pertaining to the impostor.

Six applications were from health care providers. In five of these applications, providers gave incorrect information.

### b) Significant Physical Differences Between Impostors and Victims

In two cases, impostors were a different race than their victims, but despite in-person interactions with the credit grantor, this disparity was apparently overlooked. Other significant physical differences were overlooked. X2, a Latino, is over 6 feet tall, and over 100 pounds heavier than the impostor, a significantly shorter African American. Similarly, X5 is white but the impostor is African American. X4's impostor weighed 250 pounds, but successfully masqueraded as X4 using X4's drivers license when arrested, despite outweighing X4 by 70 pounds.

### c) Fraud is Often Apparent within the "Four Corners" of the Consumer Report

Several of the ID Watchdog victims' consumer reports had obvious "intratexual" indicia of identity theft. That is, by simply analyzing the consumer report, with no extrinsic information, it should have been obvious that the fraud was present.

Several of the ID Watchdog victims had years of perfect payment history, but towards the end of their reports, one found numerous collections accounts. For instance, a summary of X4's credit score reads, "You paid 100% of your accounts on time." However, towards the end of X4's report, a reviewer would have found 20 unpaid obligations. These items that had been turned over to collections agencies indicated that X4 had never made any payment on these obligations. Similarly, X1 had a perfect payment history for legitimate accounts, but 26 delinquent, fraudulent tradelines.

---

[29] *Id.*

[30] *See generally,* Pam Dixon, World Privacy Forum, The Medical Identity Theft Information Page, http://www.worldprivacyforum.org/medicalidentitytheft.html (last visited Mar. 10, 2010).

Why would X1 and X4 faithfully pay account balances for years, and not make a single payment on others? This dichotomy between responsible and completely derelict payment could be an intratextual indication of identity theft. A study should be conducted to determine if fraud could be detected merely by reviewing consumer reports without any knowledge of the consumer or her credit activities. If this detection is possible, consumers could be automatically altered to suspicious activity on their consumer reports by consumer reporting agencies.

**d) Marginal Financial Services**

Subprime lending is present in many financial applications reviewed in this study. For instance, X5 had a good credit rating prior to becoming a victim of identity theft. The impostor applied for home loans with the following interest rates: 9.3%, 6.4%, 9.5%, and 10.5%. X2's impostor applied for a $400 loan at 126% APR.

This points to another avenue for further research: should subprime lenders suspect fraud when consumers with excellent credit apply for their products? Should that fact pattern constitute a "red flag," and if so, will subprime lenders have adequate incentives to properly vet the application if they are remunerated by fees rather than the lifetime profit from the loan?

# III. EFFICIENT IDENTITY THEFT

Recall that two paradigms have dominated the legal understanding of the identity theft problem. Lynn LoPucki frames it as a result of the modern, more private life: a decline of living in public has facilitated both the concealment of impostors and their ability to masquerade as others.[31] Daniel Solove, following a liberal privacy-control framework, argues that identity theft is a result of a broken privacy architecture, one where no one is in control of personal information. Thus, identity theft is a byproduct of a broken privacy architecture.

Much has been learned since LoPucki's first works in this field, and the factual landscape of identity theft is richer. The landscape and recent developments place strains on the LoPucki conception of the problem. For instance, LoPucki laments the decline of public life at the dawn of blogging and social networking services, on which millions of Americans are posting personal details never published in a phonebook or city directory. We seem to be entering a new era of personal revelation and disclosure about others, thus changing notions of interpersonal privacy.

But even if one accepts the idea that public identity is in decline, credit grantors do not use the sources LoPucki cites (city registers, phonebooks, and the like) for credit authentication. While privacy laws were enacted in the 1990s, credit grantors amassed databases and anti-fraud tools far richer than any phonebook or DMV database. Data brokers developed tools to aggregate a complete history of individuals' addresses, phone numbers, and other personal information.[32] Credit grantors can buy proprietary tools to help verify identity and rely upon internal databases to go beyond simply matching

---

[31] *See* LoPucki, *Privacy, supra* note 2, at 1278.

[32] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595 (2004).

application information to the credit header. In fact, never in history have so many anti-fraud tools been available to credit grantors. Thus, the LoPucki narrative describing the decline of public life misses the mark because Americans' lives are very much public to companies involved in the credit markets.

Solove frames the problem as a lack of control over personal information. No one seems to be in control, and if collection of personal information involved limits on its use and dissemination, thieves would be less likely to commandeer others' credit. LoPucki critiques the Solove approach as impractical, since there is no reliable way to selectively prevent revelation of personal information to identity thieves.[33] But the findings of the FACTA Access study suggest that, in a way, privacy-control is the root of the problem. The cases reviewed in this study show that credit grantors are willing to accept even inaccurate information on applications. This article expands the Solove critique by identifying control over credit authentication as a prime remedy to identity theft.

### A. INCENTIVES FOR QUICK CREDIT GRANTING

An extensive economic literature addresses the problem of credit risk,[34] the chance that a borrower will not pay back an obligation. However, fraud risk,[35] the chance that an impostor will open a new account, is an underexamined problem in the economic literature. Also underexamined is the complex set of incentives in the new account credit market that can be leveraged by impostors to commit identity theft.

Credit granting companies have many compelling incentives to quickly open new accounts, and in light of this, some fully automate the process. These incentives create great rewards for the granting company, and significant opportunity costs if the delay in investigating the applicant causes the customer to go elsewhere. An effective anti-identity-theft approach would consider the incentives embedded in the credit granting markets. These incentives drive credit grantors to make decisions quickly and forgo some basic identity theft prevention strategies.

Anti-fraud efforts cost money and are subject to diminishing returns, and thus credit grantors will not try to completely eliminate identity theft.[36] Even basic efforts, such as requiring an in-person interaction as recommended by LoPucki and Solove, may be very expensive in comparison to a fully-automated credit granting procedure. Writing in the UK market, Steven Finlay estimates that a mail, phone or internet application (no face-to-face interaction) costs £5-£15 to administer.[37] In store applications could cost

---

[33] *See* LoPucki, *Privacy, supra* note 2, at 1278.
[34] *See, e.g.,* Charles M. Kahn & William Roberds, *Credit and Identity Theft*, 55 J. MONETARY ECON. 251 (2008).
[35] Kahn & Roberds define fraud risk as "the risk that a debt cannot be enforced because the identity of the person incurring the debt cannot be ascertained." *Id.* at 252. Of course, with enough resources, the actual debtor's identity can be determined. Many credit grantors will not investigate impostors because of the cost involved, unless a very large fraud occurred. Thus, a better definition for fraud risk would follow standard definitions of identity theft, such as the Federal Trade Commission's, which focus upon use of another's information without authorization for some illegal purpose. 16 C.F.R. § 603.2(a) (2007).
[36] Keith B. Anderson, Erik Durbin & Michael A. Salinger, *Identity Theft*, 22 J. ECON. PERSP. 171, 182 (2008).
[37] STEVEN FINLAY, CONSUMER CREDIT FUNDAMENTALS 74 (2005).

between £20-£50.[38] Obviously, once development costs are recouped, a fully automated approval process would generate lower costs than those requiring consultation with the fraud department or manual inspection.

Decisions about anti-fraud interventions must be balanced against risk. With respect to identity theft, the overall probability of fraud is quite low. The FTC estimated that in 2005, between 1.2 and 2.8 million Americans had been a victim of new account identity theft in the previous year.[39] The total number of credit applications in the US in any given year is unknown, but could easily be in the hundreds of millions. For instance, Bank of America alone processes 14 million applications a year through automated processes.[40]

Incentive conflicts may be baked into some credit marketing arrangements. Due diligence incentives may be reduced in relationships where an issuer uses some third party, such as a telemarketer, to acquire new customers. Consider the example of the student group that receives a fee for each credit card applicant they enroll on campus. The student group is fee remunerated; if the applicant never actually uses the card or is an impostor, the student group may still profit from the transaction.

Incentives peculiar to credit granting may also cause grantors to take on more risk. For instance, the "best customer" from the credit grantor perspective could be the consumer who will charge so much that they cannot afford to pay off the balance in full in any given month. These so called "credit revolvers" are the most profitable consumers because they pay compounded interest rates on their purchases and fees.[41] However, the worst customer is very similar to the best, as a fine line divides those who charge too much and can pay the minimum balance, and those who make no payments at all. The search for revolvers provides a rational basis to seek riskier applicants who may have thinner or wemmed credit histories.

Once accounts are opened, credit grantors have found ways to mitigate the cost of fraud. I suggest that five factors create incentives to prioritize quick credit granting over stronger initial anti-fraud due diligence. These incentives are so strong that grantors have chosen to address fraud primarily through mitigating losses after credit has been extended.

First, consumers want goods and services quickly, and there are opportunity costs associated with the delays inherent in investigations of credit applications. Incentives for due diligence may be outweighed by consumer preferences and competitors with lax practices. Thus, if Bank A delays the approval of a new credit card in order to investigate

---

[38] *Id.*

[39] FED. TRADE COMM'N, 2006 IDENTITY THEFT SURVEY REPORT 1 (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[40] In a December 2007 workshop on SSNs held by the FTC, Trey French of Bank of America stated that the bank approved about 14 million credit applications a year mostly through a completely automated process, meaning that the institution had no human review of this account granting. FED. TRADE COMM'N, REMARKS AT SECURITY IN NUMBERS, SSNS AND ID THEFT 1, 82 (2007), *available at* http://www.ftc.gov/bcp/workshops/ssn/DECEMBER11.pdf.

[41] *The Secret History of the Credit Card,* PBS FRONTLINE, Nov. 23, 2004, http://www.pbs.org/wgbh/pages/frontline/shows/credit/etc/synopsis.html.

a potential fraud risk, the consumer may move along to Bank B. Often the granting of a card is paired with an immediate discount for purchases of goods. A rejected application could mean a lost sale. Credit cards, in particular, are competing with other forms of credit that take a longer time to acquire. If credit cards fail to provide instant gratification, consumers may be more willing to obtain more advantageous bank loans.

Second, awards accrue to issuers that can recruit many customers. Despite the competitiveness of credit offers, many consumers stick with the same card even when more attractive offers exist. For instance, "affinity cards" encourage lock-in to a specific card in order to give flight benefits or donations to the customer's college. This gives the credit card company "wallet space" that might be later expanded into other product offerings.

Third, while consumers directly experience fees (along with late fees, penalties, cash withdrawal fees, payment protection insurance, etc) and interest charges, other merchant fees accrue to card issuing banks. The bulk of the lucrative "interchange fee," which generates $40-50 billion in income annually mostly accrues to issuing banks.[42] In a typical $100 sale, the card-issuing bank would receive $1.80 of the $2.25 fee paid by the merchant in the sale.[43] Thus, each card issued has the potential to capture a small percentage of revenue from each sale, giving banks strong incentives to capture the largest number of consumers possible.

Fourth, electronic payment increases "spend," meaning that consumers, divorced from the experience of parting with cash, are generally willing to spend more money on credit. Converting consumers from cash to credit results in more revenue in real dollars, but also fees from each sale.

Once an account is opened, credit issuers have found many ways to mitigate financial risks from identity theft. For instance, in some cases, liability for fraudulent charges is imposed upon merchants. A recent report by LexisNexis finds that merchants absorb $100B in losses annually because of identity theft, while financial institutions lose about $11B.[44] Consumers have been known to pay fraudulent charges in order to clear their credit report. LexisNexis estimates that consumers absorb almost $5B annually. Credit issuers can securitize credit card debts, and thus spread the risk of fraud among different investment vehicles, depending on investors' appetite for risk.[45] Finally, fraud losses are written off as business losses, and thus can offset tax burdens.

Credit issuance can be extremely lucrative, and because of customer biases and behavior, a successful issuer will attempt to obtain as many new accounts as possible. Risk of fraud can be mitigated, while risk of losing business to faster acting competitors cannot.

---

[42] Andrew Martin, *Card Fees Pit Retailers Against Banks*, N.Y. TIMES, July 16, 2009, at B1.
[43] *Id*.
[44] JAVELIN STRATEGY & RESEARCH, LEXISNEXIS, TRUE COST OF FRAUD STUDY 1, 14-23 (2009), *available at* http://risk.lexisnexis.com/literature/LexisNexisTotalCostFraud_09.pdf.
[45] Kathy Chu & Byron Acohido, *Why Banks are Boosting Credit Card Interest Rates and Fees*, USA TODAY, Nov. 14, 2008, *available at* http://www.usatoday.com/money/industries/banking/2008-11-09-bank-credit-card-interest-rates_N.htm?loc=interstitialskip.

Recall that LoPucki links the rise of identity theft to the perception that we live more private lives. Contrary to LoPucki's observations, credit grantors have more personal information today than ever, but this study shows that when impostors make errors in applying for credit, grantors override or ignore those errors. Thus, this is not a problem of public or private lives or the availability of information, it is a problem of business decisions to prioritize new account generation over due diligence.

In light of the FACTA Access Study results and of the incentives in credit granting, the advance of automated credit granting systems provides a better explanation for the identity theft problem. The "miracle of instant credit," the ability of anyone almost anywhere to apply for and obtain a new account in seconds, has a dark underbelly -- the miracle of instant identity theft. It allows impostors to be instantly rewarded for their crimes, with little risk of arrest or prosecution. Its rise in the 1990s offers a far more compelling explanation of the modern identity theft problem.

# IV. INTERNALIZING THE EXTERNALITIES

This section reviews the interventions proposed by LoPucki and Solove. Then, two alternative regulatory approaches are discussed: the newly promulgated Red Flag Rule and a proposal to fix the underlying incentives driving the problem.

## A. WHAT WOULD LOPUCKI & SOLOVE DO?

Despite their different paradigms, LoPucki and Solove agree on several identity theft interventions. Both agree that the SSN should not be used as an authenticator.[46] This means that credit grantors should not use knowledge of the SSN as proof of identity. Both agree that new credit applications should require an in-person interaction.[47] Both agree that consumers should be notified proactively of credit activity.[48]

At that point, the two diverge. LoPucki articulates a voluntary system where individuals can claim their identities, mediated through a trusted government agency, such as the department of motor vehicles.[49] Once one's identity is claimed, the individual could be more involved in the credit authentication process.

These interventions may reduce the incidence of identity theft, but they largely miss the incentives that are driving the identity theft problem. LoPucki and Solove attempt to address specific vectors that enable the crime, such as use of the SSN as an authenticator, and to harden the institutions currently used to commit the crime. But even if grantors are prohibited to use the SSN as an authenticator, the results of the FACTA Access study suggests that the incentive structure may still drive risky credit granting.

In-person credit application mandates suffer from several different problems. First, such an approach would create a great burden for both consumers and merchants. Internet credit transactions, and newly emerging instant credit products would likely not be profitable if costly personal visits were required.

---

[46] LoPucki, *Privacy, supra* note 2, at 1279; Solove, *supra* note 7, at 1270.
[47] LoPucki, *Privacy, supra* note 2, at 1279.
[48] *Id.*
[49] *See generally* LoPucki, *Human Identification Theory, supra* note 2.

More importantly, in-person interactions may not be very effective in reducing fraud. Such a mandate assumes that cashiers and store employees will be able to recognize impostors as such. These employees will have to be trained to look for data mismatches between what is presented on the application and on credit headers, to recognize fake credentials, and even to determine when someone is posing as another using a real credential. Generally speaking, many people are not proficient at these tasks. As any college student can attest, using a friend's drivers license to gain entry to a bar is usually as simple as having the same hair color.

The results of the FACTA Access study also suggest that in-person meetings would not have been very effective in reducing fraud. Impostors were authenticated as the victim in cases where significant physical differences were present, and even where the impostor and victim were different races. Furthermore, several impostors had either fabricated or real state-issued identity cards.

Proactive notice of credit activity would not prevent identity theft, but it would reduce the impact of the crime. Several studies have shown that early detection of fraud reduces harm to victims. Still, such a requirement would result in the dispatch of hundreds of millions of notices annually in cases where no fraud was present, in order to make individuals aware of 2-3 million actual cases of fraud.

## B. THE RED FLAG RULES APPROACH

Anecdotally, the problem of sloppy credit granting has been well documented. The FACTA Access study is the first to empirically demonstrate a problem, albeit, with a small sample of six victims of new account identity theft. As explained above, Congress included the Red Flags Rule mandate in the passage of FACTA in 2003. This mandate reflected a need to require better practices in the authentication process.

It would seem that the Red Flag approach would be effective in addressing the problems found in the FACTA Access study. Among 16 fraudulent applications presented by impostors to obtain credit from 1999-2007, one finds that credit grantors have extended new accounts despite the presence of basic contact information errors on the applications. This credit granting behavior fits squarely within the sample red flags specified by federal agencies. For instance, the regulations specify that a notice of an address discrepancy provided by a consumer reporting agency qualifies as a red flag. Three of X5's mortgage applications included address discrepancy notices, but the mortgages were extended anyway. Similarly, the regulations specify that when an applicant presents an address not currently in the consumer's report, a red flag is raised.

The Red Flag Rules also speak to physical differences between the applicant and the victim. Two cases concerned victims who were of a different race than their impostor. Outside the credit granting context, two cases involved significant weight differences between impostor and victim.

But will the Red Flag Rules be effective in practice? The mandate follows a very extended period of rulemaking--the Red Flag Rules were not issued until October 2007,[50]

[50] FED. TRADE COMM'N, AGENCIES ISSUE FINAL RULES ON IDENTITY THEFT RED FLAGS AND NOTICES OF ADDRESS DISCREPANCY (Oct. 31, 2007), *available at* http://ftc.gov/opa/2007/10/redflag.shtm.

and covered entities were given a full year to comply. However, once its effective date of November 2008 arrived, an extension was granted for compliance.[51] Credit grantors received the Rules with a collective groan. It became clear that by the November 2008 implementation date, there would be widespread non-compliance, both because of confusion over the Rules, but also because of a lack of alacrity among banks to implement them.

Credit grantors are given very broad discretion to respond to red flags. They must simply make "appropriate responses" to the red flags "commensurate with the degree of risk posed."[52] Thus, there is a risk that credit grantors will spot red flags, and apply weak "appropriate responses" that still result in a new account issued. For instance, in X5's case, consumer reporting agencies alerted the grantor to significant information discrepancies, but new accounts were still issued.

More importantly, because of incentives to quickly grant credit, issuers are not likely to identify new red flags. Identifying new red flags could hurt their ability to obtain new customers, because different grantors can develop their own indicia of fraud. Grantors that decide not to implement many red flags will be able to open new accounts more quickly than those that diligently comply with the regulation.

The FTC and banking agencies responsible for the Red Flags Rule can identify indicia of fraud that all credit grantors must follow. However, operating from outside the industry, the agencies are unlikely to be on the vanguard of fraud trends. As it has been in the past, agencies will develop new red flags in response to anecdotal information, especially tales of sloppy credit granting exposed in the media. Without the insight that fraud analysts obtain from datamining and years of experience in detecting fraud, agency-developed red flags are likely to lag behind, and once proposed, subject to intense lobbying campaigns to prevent changes to the rule, and to delay their implementation.

Simply put, if ignoring red flags or complying with the minimum mandated care is more expensive than tolerating fraud (and thereby acquiring more customers than a competitor), its incidence will not be reduced. Identity theft will still be rampant, and victims will still be uncompensated for the externalities of the crime.

The Red Flags Rule shares the same core problem as the LoPucki and Solove approaches: it does not address the underlying thirst for customer acquisition that drives high risk tolerances. A more effective approach would put a thumb on the economic scale that would encourage the marketplace towards more responsible practices.

### C. NEGLIGENCE AND STRICT LIABILITY APPROACHES

How the law should address the identity theft externality is a complex problem. Credit is essential to our modern economy. Barriers to access can stall the economy and darken the financial futures of all. At the same time, public policy norms that prioritize quick access to credit -- à la the "miracle of instant credit" evangelists -- have

---

[51] FED. TRADE COMM'N, FTC WILL GRANT SIX-MONTH DELAY OF ENFORCEMENT OF 'RED FLAGS' RULE REQUIRING CREDITORS AND FINANCIAL INSTITUTIONS TO HAVE IDENTITY THEFT PREVENTION PROGRAMS (Oct. 22, 2008), *available at* http://www.ftc.gov/opa/2008/10/redflags.shtm.

[52] Identity Theft Rules, 16 C.F.R. § 681, app. A (2009).

unintentionally encouraged a landscape ripe for fraud. Overreaction in the direction of restricting credit, or in encouraging its extension to anyone both are fraught with peril.

I argue that existing solutions to the identity theft problem have been too narrowly focused on particularly irresponsible practices among credit grantors. These approaches risk creating reification as credit grantors focus on complying with prescriptive rules. Further, highly regulated institutions operating in a compliance mindset are likely to follow the letter of the law rather than effectuate its purpose of reducing identity theft.

More attention is needed to the underlying incentives that drive sloppy credit granting. Identity theft is an externality that is the product of instant credit. And creditors control the instant credit valve. They can open it fully, or narrow it, by implementing greater controls. The FACTA Access Study shows that consumers cannot prevent this crime, because creditors are willing to accept even incorrect information in authenticating customers. The answer therefore is to align incentives, so that the costs currently accruing to millions of consumers fall back upon credit grantors.

Some commentators have suggested that credit granting institutions be subjected to suits in negligence for identity theft. Anecdotal evidence, and the participants in the FACTA Access Study suggest that credit grantors are overlooking disconfirming evidence in credit granting decisions. Sloppy procedures could be viewed as negligent behavior, with lawsuits for damages serving as an incentive to improve practices. Heather Howard has suggested this approach:[53]

> When financial institutions act negligently, they jeopardize the financial well-being of the individuals whose information they manage. Because a quasi-relationship arises between a financial institution and an individual in whose identity it opens an account, the institution should be responsible in tort for the consequences of its negligent actions or failures.[54]

Howard acknowledges that the traditional tort requirements of showing duty, breach, causation, and damages will be challenging for plaintiff/victims of identity theft. In the new account identity theft context, duty has proven to be the highest hurdle for litigants pursuing negligence theories. Credit issuers argue that they have no legal duties to non-customers, and that in any case, they should not be liable for the criminal actions of third party impostors.[55]

Credit issuers have had some success with these arguments. In a survey of negligence cases, David Szwak observes:

> These cases illustrate that a plaintiff seeking to recover against a bank or credit issuer following an identity theft must carefully plead and prove facts to support a negligent enablement or similar claim. Obviously a pre-existing relationship and duty . . . is helpful to the plaintiff and may even

---

[53] Heather Howard, *The Negligent Enablement of Imposter Fraud: A Common-Sense Common Law Claim*, 54 DUKE L.J. 1263, 1283 (2005), *available at* https://www.law.duke.edu/shell/ cite.pl?54+Duke+L.+J.+1263.

[54] *Id*. at 1283.

[55] Huggins v. Citibank, N.A., 585 S.E.2d 275 (2003).

> be essential. . . . [M]ost courts do not recognize a general fiduciary duty to the public on the part of banks or other business enterprises. Thus a separate relationship and duty . . . or perhaps under the FCRA, appears to be a requisite for recovery in most identity theft cases.[56]

Brendan Delany suggests that this limitation could be surmounted, if courts were willing to assume that identity theft is a foreseeable risk of negligent issuance of credit cards:

> By employing "liability beyond the risk," courts can establish a legal duty for an issuer of credit cards to confirm applicants' identities. "Limitation of liability to the risk" [requiring the plaintiff to prove that identity theft was foreseeable] enables CRAs [consumer reporting agencies] and banks to disseminate personal information and issue credit cards without serious inquiry or proof that the consumer is in fact who he or she claims to be. Indeed, the Polzer court refused to hold the bank liable "even when they failed to take any steps whatsoever to confirm the applicant's identity and where they could have easily and inexpensively done so." "Liability beyond the risk" will impose a greater duty on CRAs and creditors to exercise greater care and thus significantly reduce the possibility of identity theft.[57]

Still, the negligence approach's other hurdles present challenges to plaintiffs. Writing in the context of database security, Danielle Citron considers and rejects a negligence approach for addressing leaks of personal information.[58] Citron's analysis of an analogous situation is useful here. Citron considers the duties of companies that hold massive databases against leakage, which can take the forms of both accidental spills, and the intentional acts of malicious hackers.[59] Clearly, databases of personal information have much social utility; just as credit granting has provided economic development and social mobility. Quick credit granting could not even be possible without the databases that Citron describes, yet, like access to credit, these databases must be carefully managed to prevent harm to many people.

Citron argues that a negligence approach fails from both economic and moral perspectives. Economically, a negligence regime could create inefficiency, because uncertainty would surround the optimal level of care to prevent leaks of personal information.[60] In the context of sloppy credit grant systems, this threat loom large. Credit grantors may overreact by requiring burdensome authentication measures. This could result in a slowdown in credit issuance, leading to missed opportunities.

---

[56] David Szwak, *Update on Identity Theft and Negligent Enablement*, 58 CONSUMER FIN. L.Q. REP. 66, 71 (2004).
[57] Brendan Delany, *Identity Theft: The Fair Credit Reporting Act and Negligent Enablement of Impostor Fraud*, 54 CATH. U. L. REV. 553, 586 (2005) (citations omitted).
[58] Danielle Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 261-68 (2007).
[59] *Id.* at 243-46.
[60] *Id.* at 263-64.

Individuals with "thin" credit files or limited identity credentials may shut out of the credit markets.

Uncertainty would also lead to "battles of the experts" on credit granting procedures. The FACTA Access Study provides examples of what appears to be negligent credit granting.[61] Consider the example of the situation where the impostor provided an address at which the victim never lived. Is it not sometimes reasonable to open an account to an individual at a new address? In this situation, even if the credit grantor uses a commercially available database s to verify the address, a new address may not appear in the database for some time. What verification would be effective in such a circumstance?

Citron further identifies management of "residual risk" as problematic.[62] A negligence regime would leave victims uncompensated where due care was exercised, but a data leak occurred nevertheless.[63] Similarly, in the identity theft context, credit grantors will argue that their anti-fraud systems were sufficient, and although credit was granted, that in itself does not demonstrate negligence.[64] Consumers thus will be uncompensated for the harms related to beneficial economic activity over which they can neither exercise control nor profit from.

After rejecting negligence as a basis for liability in addressing database security, Citron turns to strict liability, using the example of ultrahazardous activities.[65] Citron leverages the seminal case of *Rylands v. Fletcher*[66] as a model.[67] *Rylands* considered the duty of care to safeguard water reservoirs.[68] Water reservoirs are socially useful and necessary, but can cause extraordinary damage if breached, by accident, negligence, or intentional action. The *Rylands* court's extension of liability without fault for their breach, and the subsequent acceptance of this approach in the US, offers a model for managing risks of database leakage, according to Citron.[69]

Strict liability will provide more efficiency, because database providers have ultimate control over use of personal information and protections that are in place:

> Database operators constitute the cheapest cost avoiders vis-à-vis individuals whose information sits in a private entity's database. Database operators have distinct informational advantages about the vulnerabilities in their computer networks. Individuals, by contrast, cannot detect and understand the security offered by information brokers, employers, colleges, or biometric vendors. . . . [and] the database operator sits in the

---

[61] *See supra* Part II.B (revealing that credit granters approve applications with false addresses, false phone numbers, incorrect dates of birth, false social security numbers, and the wrong drivers license number).
[62] Citron, *supra* note 58, at 264-67.
[63] *Id.*
[64] Beard v. Goodyear Tire & Rubber Co. 587 A.2d 195, 201 (D.C. App. Ct. 1991).
[65] Citron, *supra* note 58, at 268-77.
[66] Rylands v. Fletcher, 3 L.R.E. & I. App. 330 (1868).
[67] Citron, *supra* note 58, at 270-71.
[68] *Id.*
[69] *Id.* at 278-80.

> best position to make decisions about the costs and benefits of its information-gathering.[70]

The FACTA Access Study indicates that consumers have no control over the credit authentication process taking place between grantors and imposters.[71] Even if a consumer invests time and money in avoiding revelation of personal information, some credit grantors will issue new accounts to impostors with incorrect personal information. There is no way to opt out of the credit markets -- even toddlers' identities are stolen in the current situation. The cheapest cost avoider in the identity theft context, thus is the credit issuer. The relationship is so asymmetric that the individual is literally at the mercy of the risk preferences of companies with which no relationship has even been established.

Residual risks would be addressed by a strict liability regime. In a discussion directly relevant to poor authentication in identity theft, Citron continues to explain why insurance does not offer a remedy to consumers:

> Experts report that identity-theft insurance is not "worth the money" because it does not cover direct monetary losses incurred as a result of such theft. On the other hand, database operators can most efficiently spread the costs of data leaks by obtaining a single cyber-risk insurance policy as opposed to the countless identity-theft insurance policies obtained by individuals.[72]

Indeed, as recounted in section III above, credit issuers have a number of strategies to mitigate financial lost because of identity theft. However, consumers have no reasonable strategies to address the harms of the crime, whether or not the credit grantor was negligent.

Given that credit grantors are in control of the new account identity theft problem and that credit grantors can manage risks related to that control while consumers practically cannot, a strict liability approach may create a more efficient allocation of costs among credit grantors and victims of identity theft. Presumed damages could be awarded, keyed to the average time that consumers spend remedying the crime. Statistics on average time and related cost to consumers are closely tracked by the FTC and by private parties, thus making it possible to place a certain value on a claim, even if the victim cannot show specific economic harm. Victims who can show economic damage, for instance, through lost opportunity and the like, would be able to plead those damages and recover.

# V. CONCLUSION

Throughout the 1990s and 2000s, lawmakers and regulators were urged not to create rights and responsibilities in personal data, because, among other things, it was

---

[70] Id. at 284-85 (citation omitted).
[71] *See supra* Part II.B (revealing the ease with which imposters can use only fragments of personal information to secure credit).
[72] *Id.* at 285 (citations omitted).

feared that privacy law would make anti-fraud efforts more difficult.[73] Congress largely heeded this advice, giving wide berth of anti-fraud uses of personal information. This, of course, is a common narrative in the privacy world: individuals trade off having rights and responsibilities in data because it is believed that we all will be more secure if data can be used for anti-fraud purposes.

This article has elucidated an unfortunate irony in this narrative: policymakers chose to leave many anti-fraud uses of data free from consumer privacy laws, and yet, identity fraud continues to affect almost ten million Americans each year. In analyzing 16 applications pertaining to 6 victims of identity theft, it is clear that the most basic anti-fraud tools would have spotted errors impostors made when masquerading as the victims. For instance, X5's impostor was using the wrong date of birth and an invalid drivers license number -- one never issued by the state. We are in an unfortunate situation where consumer privacy was subordinated to anti-fraud interests, and the very people who said it was important to have anti-fraud tools could not care to use them, or perhaps even worse, they used them and ignored signals that fraud was present.

Proposals to mitigate identity theft remain narrow, focused upon particularly troubling practices may be limited in effect. Incentives are at the core of the identity theft problem. More money can be made by tolerating high levels of fraud than by more carefully screening against impostors. The market rewards lax authentication practices, because market actors risk losing new customers to competitors if they delay transactions to prevent fraud. Identity theft is an externality of the instant credit marketplace. Consumers have no ability to control whether they are a victim of this externality, because consumers are not in control of credit authentication.

An effective approach to reducing the incidence and impact of identity theft would address the underlying incentives that drive the instant credit market. If credit grantors, the entities that enjoy the great fruits from quick access to credit, were fully liable for its costs, more care would be applied to protect individuals from identity theft. A negligence regime could shift these costs, but could also produce suboptimal outcomes. However, a strict liability approach would simplify the remedial process for victims, and create stronger, direct incentives to prevent fraud.

---

[73] Anti-fraud systems need not depend on personal information. For instance, German researchers have found that analysis of basic demographic information is highly effective in segmenting accountholders into different fraud buckets. Thomas Hartmann-Wendels, Thomas Mählmann & Tobias Versen, *Determinants of Banks' Risk Exposure to New Account Fraud – Evidence from Germany*, 33 J. BANKING & FIN., 347 (2009).