The Credit Industry and Identity Theft: How to End an Enabling Relationship

Eric T. Glynn
University at Buffalo School of Law (Student)

Follow this and additional works at: https://digitalcommons.law.buffalo.edu/buffalolawreview

Part of the Banking and Finance Law Commons, and the Criminal Law Commons

Recommended Citation
Available at: https://digitalcommons.law.buffalo.edu/buffalolawreview/vol61/iss1/6
COMMENT

The Credit Industry and Identity Theft: How to End an Enabling Relationship

ERIC T. GLYNN†

INTRODUCTION

"An ounce of prevention is worth a pound of cure." - Benjamin Franklin

The popular Web comic xkcd recently ran a strip featuring a man in a military-style cap, sitting at a computer, using an—apparently Web-based—missile launch program.1 The program first asks the man for the target's coordinates, and then for his e-mail address.2 In the final frame, the program asks the man to retype his e-mail address for verification.3 Playing on this theme in the accompanying text, the author, Randall Munroe, muses: “I hear in some places, you need one form of ID to buy a gun,

† J.D. Candidate, Class of 2013, SUNY Buffalo Law School. I would like to thank Professors Patrick J. Long and S. Todd Brown for their helpful suggestions, and everyone at the Buffalo Law Review for their hard work.

2. Id.
3. Id.
but two to pay for it by check. It’s interesting who has what incentives to care about what mistakes.”

Although Munroe’s missile program is obviously a joke, his gun remark could literally be true: federal law only requires one form of identification for a firearm purchase, but retailers may require more from a check-writer due to the propensity for fraud or insufficient funds to render the check worthless. Regardless, he invokes a well-established precept of economics and tort: often, reasonable precautions will not be taken unless the actor has an incentive to act, or bears a cost for inaction. In the comic, the proprietor of the fictional missile launch program has an economic incentive in ensuring the e-mail address is correct, as the e-mail address is a tradable commodity. The accuracy of the location about to be destroyed by a missile, however, is someone else’s problem. The failure to make even a modest effort to ensure the correct target is acquired, in an environment in which any such measures may be life-saving, comes with no price tag attached. And so, without an appropriate economic disincentive, the actor that is in

4. Id.

5. Federal law only requires one form of ID to purchase a gun. See 18 U.S.C. § 922(s)(1)(A)(i)(II) (2006 & Supp. V 2011) (referring to “the” identification document presented before a transfer of a firearm, implying only one is required). Meanwhile, many businesses are very strict about who they accept checks from, for the reasons mentioned, so it is conceivable that a business, such as a gun shop, might require two forms of identification for its customers paying by check, despite only requiring one to merely purchase the firearm.

6. See Richard A. Posner, A Theory of Negligence, 1 J. LEGAL STUD. 29, 33 (1972) (“If . . . the benefits in accident avoidance exceed the costs of prevention, society is better off if those costs are incurred and the accident averted, and so in this case the enterprise is made liable, in the expectation that self-interest will lead it to adopt the precautions in order to avoid a greater cost in tort judgments.”).

7. A consumer’s e-mail address has become, in many ways, his online identity. Cf. Lenny Zeltser, Why On-line Social Identity and Reputation is a Big Deal, LENNY ZELTSER ON INFO. SEC. (Nov. 3, 2010), http://blog.zeltser.com/post/1470112351/social-identity-reputation. Online entities value this information for a number of reasons, ranging from perfectly reasonable (having a way to reset a password), to annoying (soliciting their customers with information about their products or services), to troubling (creating a personality profile with aggregate user data), to illegal (reselling the addresses to unsolicited marketers or “spammers”).
the best position to safeguard against disaster has very little reason to.

Such is the present state of the consumer credit industry. Despite being in existence for over 100 years,

8 it is fraught with fraud because those most integral to the process often do very little to avert it.

9 Indeed, identity theft would often be preventable if creditors and consumer reporting agencies (“CRAs”) adopted some what seem to be common sense standards of verifying that credit applicants are who they claim to be.10 Meanwhile, credit has become, more and more, an individual’s economic lifeblood: good credit is required for everything from renting a car to getting a job.11 As it stands, however, the credit industry has little incentive to adopt preventative measures, as it has been difficult for consumers to hold creditors and credit bureaus accountable for their lapses in care.12 This dearth of recourse for identity theft victims is the result of a frustrating combination of congressional clumsiness and judicial indifference.13 While Congress has, over the past four decades, enacted some important legislation in its attempt to provide consumer credit protection, these measures have ranged from incomplete to completely toothless.14 Courts, in the wake of such disjointed guidance, have been cool toward allowing claims against the credit industry to proceed, regardless of whether those claims are based in federal, state, or common law.15 Thus, despite an

8. Equifax was established in 1899 as “Retail Credit.” Simson Garfinkel, 
9. See infra Part I.C.
10. See infra Part II.B.1.
11. See infra Part I.D.
12. See infra Part II.
13. See infra Part II.B.2.
14. See Krista A. Dotson, Note, Your Good Name: Identity Theft and the Consumer—A Casenote of Andrews v. TRW, Inc., 22 QUINNIPIAC L. REV. 611, 613 (2004) (“Although a myriad of legislative measures addressing identity theft and privacy issues are available to the personal consumer, the legislation, in its current form, can only be described as ‘piecemeal’ or ‘reactionary.’”); infra Part II.B.2.
15. See infra Part II.B.
increase in criminal convictions, identity theft victims have found the legal system perplexingly hostile to their claims, leaving them uncompensated and—worse—leaving intact a credit system that facilitates fraud.

That is why this Comment advocates a legislative and judicial attitude adjustment in favor of better protecting consumers and their increasingly important credit. Legislatively, Congress need only make some minor improvements to give teeth to existing consumer credit rights. Judicially, courts need to recognize the legal bases upon which a victim may sue creditors and CRAs: The Fair Credit Reporting Act (“FCRA”) and common-law negligence. In either instance, relatively small common-sense changes are all that’s required to finally force the credit industry to stop playing fast and loose with consumers’ information and to finally stop identity theft before it occurs.

Part I discusses what identity theft is, how the credit industry operates, how that operation leads to identity theft, and how this fraud harms victims. Part II outlines the various culpable parties in a given identity theft case (creditors, CRAs, and the identity thieves themselves), what role they play in identity theft, and how they have been largely exonerated from victims’ claims against them by an unsympathetic legal system. Finally, Part III explains how the law, particularly considering recent developments, could allow for recovery against creditors and CRAs who negligently compromise consumers’ identities, and how, at long last, we might allow identity theft victims a real means of recovery for the harm they suffer, and finally stem the tide of identity theft.

I. Background

A. What Is Identity Theft?

What this Comment refers to as identity theft is actually a subset of the larger concept of misappropriating


17. See infra Part II.
someone’s personal information for a dishonest purpose. The identity theft at issue here is “true name fraud,” where a thief uses a victim’s personal information to open a new account.\textsuperscript{18} Other forms of identity theft include “account takeovers,” where a thief uses an existing credit account without the victim’s consent,\textsuperscript{19} and “criminal identity theft” where a person accused of a crime gives a victim’s information instead of their own to avoid repercussions of conviction.\textsuperscript{20} These instances, while regrettable and certainly damaging to victims, already to a large extent have preventative measures in place,\textsuperscript{21} as well as predictable remedies,\textsuperscript{22} and are thus beyond the scope of this Comment.

In true name identity theft, a perpetrator acquires the victim’s personal information through any variety of means: dumpster diving, stealing mail, misappropriating employee information, phishing scams, and countless others.\textsuperscript{23} And while better protection of that personal information is certainly one means to combat identity theft, in a world where information is shared so easily and required for so many transactions, the ability to effectively seal off one’s personal information from any potential threat is nearly


\textsuperscript{19} Id. at 851.

\textsuperscript{20} Mignon M. Arrington, Establishing Appropriate Liability Under the Fair and Accurate Credit Transactions Act, 15 N.C. BANKING INST. 357, 358 n.7 (2011).

\textsuperscript{21} Law enforcement officials, unsurprisingly, take many measures to ensure an individual’s identification, checking government identification, and later fingerprinting and photographing a suspect. See John N. Ferdico, Henry F. Fradella & Christopher D. Totten, Criminal Procedure for the Criminal Justice Professional 346 (10th ed. 2009).

\textsuperscript{22} For example, federal law prohibits credit card companies from holding a consumer responsible for unauthorized charges if reported missing before misuse, preventing any damage to his or her credit. See Fed. Trade Comm’ n, Credit, ATM, and Debit Cards: What to Do If They’re Lost or Stolen, FTC Facts for Consumers 1 (June 2002), http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre04.pdf.

impossible. Our personal information is used in any number of daily transactions and is actively collected and stored in countless databases. This is done not only by government entities and CRAs, but by commercial data mining organizations who sell (portions of) the information to other commercial interests hoping to learn more about their target demographics. As Professors Robert Sprague and Corey Ciocchetti warn:

The amount of personal identifying information collected in modern life is vast: transactional data is tracked, cell phones are monitored, Web surfing is recorded, and our moves in public are recorded by surveillance cameras. “The small details that were once captured in dim memories or fading scraps of paper are now preserved forever in the digital minds of computers, vast databases with fertile fields of personal data.” “Individually, each of these pieces of personal information represents a mere pixel of [someone’s] life, but when pieced together, they present a rather detailed picture of [that person’s] identity.”

This ubiquity of personal information means there is an abundance of opportunity for a consumer to have his identifying information compromised. Whether by a third-party’s malicious infiltration or by an entity’s improper handling, data breaches are exceedingly common: “[B]usinesses, financial groups, educational institutions, government entities, and medical healthcare groups have all reported unauthorized access of personal data.”

24. See Raymond G. Mullady, Jr. & Scott D. Hansen, Identity Theft Litigation: A Roadmap for Defense and Protection, UTAH L. REV. 563, 564 (2008) (“Technological innovation has facilitated the efficient creation, transmission, and storage of substantial amounts of information, including consumers’ credit histories, financial records, and other personal identifying information. . . . Online shopping, online banking, and other transactions can be completed over the Internet. In addition to the Internet, computerized databases and networks allow companies to maintain computerized customer information and data that further enhances the utility of commerce—both online and over-the-counter. But the development of consumer credit in our nation’s economy has unfortunately opened the door to identity theft.”).


26. See id.

27. Id. at 95 (citations omitted).

28. Id. at 97.
stronger standards protecting consumer data are clearly needed, from a practical standpoint, misappropriation and misuse of personal information is almost inevitable. As such, we are all potential victims of identity theft.

On a much more trivial note, this Comment will use the phrase “identity theft” instead of alternate terms like “identity fraud” or “imposter fraud.” Despite not being technically sound, this phrasing dominates the legal and media landscape, and so I use it in an attempt to enhance clarity. I defend my choice because the term “identity theft” has caused some consternation among certain members of the judiciary. This Comment will also sometimes refer to perpetrators of identity theft as “identity thieves” for reasons of linguistic simplicity.

B. What Is the Credit Industry?

The credit industry, or at least the credit industry to which this Comment refers, is a vast informal association of creditors—such as banks, financial institutions, credit card companies, utilities, and service providers—and credit bureaus, also known as consumer reporting agencies or CRAs. These definitions are consistent with those provided in Title 15, Chapter 41 on Consumer Credit Protection of the United States Code. See 15 U.S.C. § 1681a(e) (2006) (“The term “creditor” means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.”); 15 U.S.C. § 1681a(f) (2012) (“The term “consumer reporting agency” means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or
open credit accounts with them, offering either cash or services now in exchange for payments, usually subject to interest, later. Consumers must apply for these credit accounts, a process that almost invariably consists of the creditor purchasing the consumer's credit report from one of the three major CRAs: Experian, Equifax, or TransUnion. A credit report is an agglomeration of a consumer's information, but is primarily concerned with previous credit accounts and payment history. If that report is favorable, and its corresponding "credit score" is high enough, the creditor will grant credit to the consumer, and the consumer may almost immediately begin obtaining cash, goods, or services, and charging them to his or her account. The appeal of this kind of arrangement to consumers is immense: as of May 2011, United States consumers carried a whopping $2.44 trillion in debt. Of that total, $795.9 billion is revolving debt, an open line of credit that is paid off in installments, a category that refers almost exclusively to credit cards.

C. How Does the Credit Industry Facilitate Identity Theft?

Creditors feed off this consumer desire for instant gratification and as a result have great incentive to make access to credit as simple as possible. Thus, opening a facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

35. Id. at 3, 9.
36. Id. at 3.
37. See id.
38. See id. at 3.
41. See Heather M. Howard, The Negligent Enablement of Imposter Fraud: A Common-Sense Common Law Claim, 54 DUKE L.J. 1263, 1282 (2005) (“In a competitive market, these institutions fear that a more rigorous screening
credit account requires very little consumer information: a full name, address, birthdate, social security number, and a few questions about your income will satisfy an application for most credit cards.\textsuperscript{42} Identification or other verification of identity is seldom required;\textsuperscript{43} in fact, the entire process is done with increasing frequency online.\textsuperscript{44} Often, creditors will even send out attractive “pre-approved” credit applications to consumers based on their credit metrics.\textsuperscript{45} Unfortunately, this environment of “easy credit” means easy identity theft as well.\textsuperscript{46} As very little information is required to obtain credit, an identity thief can open numerous fraudulent accounts with information as basic as a social security number matched with an approximate name and birth date.\textsuperscript{47} Other information, such as employer, income, and address, can often be fabricated completely.\textsuperscript{48}

Long-postponed regulations requiring creditors to establish procedures for verifying identity have hitherto produced no noticeable effect. Federal law has also required CRAs for years to make reasonably certain the applicant is who he claims to be.\textsuperscript{49} Yet CRAs, which actually keep records of this supplemental information, will still often provide a credit report to a creditor even if the applicant’s supplemental information is incongruous, as long as the basic information is the same or largely similar to their process might scare consumers away to competitors who do not take such measures.\textsuperscript{7}).


\textsuperscript{43} See id. (not requiring any further identification).

\textsuperscript{44} See Sprague & Ciocchetti, supra note 25, at 94-96.


\textsuperscript{46} Although the financial downturn has reduced the number of credit offers, this shift has not produced any noticeable difference in the level of scrutiny given to the remaining accounts opened. See Barbara Kiviat, The Credit Crunch: Where Is It Happening?, TIME BUS. (Sept. 30, 2008), http://www.time.com/time/business/article/0,8599,1845818,00.html.

\textsuperscript{47} See infra notes 83-84 and accompanying text.

\textsuperscript{48} Id.

\textsuperscript{49} Cf. infra Part II.B.2.
This is because CRAs make money by selling these consumer credit reports to potential creditors, and creditors make money by maximizing the number of credit accounts they open. Thus, their incentive to continue to operate in this careless fashion outweighs any consideration of possible liability, particularly when such liability has been seldom enforced.

In the absence of any meaningful reason for the modern credit industry to try to prevent it, identity theft is rampant. In the year 2005, 8.9 million people were victimized by identity theft. By 2009, that number had increased to 11.1 million people, meaning that nearly 5% of the United States population had been victimized by identity theft over the course of a single year. Clearly, the current methods of discouraging identity theft have fallen short. And while there is certainly enough blame to go around, the lack of accountability placed upon the credit industry to take measures to prevent this phenomenon, when it is well within their power to do so, cannot be sustained.

D. Who Suffers the Consequences of Identity Theft?

Today, most Americans have either been affected by identity theft themselves or know someone (and probably several someones) who has. Once affected, a victim finds himself or herself in a financial and legal mess that is, at best, a major inconvenience to clean up, or at worst, a life-

50. See infra note 146 and accompanying text.
51. Javelin Study, supra note 16.
52. Id.
53. For example, individuals and businesses can and should better safeguard personal information. See Sprague & Ciocchetti, supra note 25, at 91; see also FED. TRADE COMM’N, GETTING CREDIT, supra note 34, at 13. Also, the FBI and other law enforcement agencies might make battling identity theft a higher priority, as the DOJ and FBI have been notably sliding back combative efforts. See Tony Romm, Report: Fast-growing crime of identity theft has ‘faded’ as DOJ, FBI priority, THE HILL (Mar. 31 2010, 9:27 AM), http://thehill.com/blogs/hillicon-valley/technology/90007-report-identity-theft-has-faded-as-doj-fbi-priority.
54. I am making a reasonable inference based on studies that have shown millions of Americans are affected each year, so that certainly cumulatively by now the effects of identity theft are very familiar to the average American. See Javelin Study, supra note 16.
altering experience. This is due to incredible importance of good credit in an increasingly credit-dependent economy: today, it is required to do everything from renting a car to getting a job.\textsuperscript{55} An individual can spend years trying to reclaim his or her good name, meanwhile suffering from the stigma of bad credit that may include denial of services, loans, and employment, as well as humiliation and even arrest.\textsuperscript{56} A recent FTC publication confirms that:

People whose identities have been stolen can spend months or years—and thousands of dollars—cleaning up the mess the thieves have made of a good name and credit record. . . . \textsuperscript{56} Victims of identity theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they didn't commit. Humiliation, anger, and frustration are among the feelings victims experience as they navigate the process of rescuing their identity.\textsuperscript{57}

Individual victim's stories range from regrettable to horrifying. Many merely spend a substantial amount of time and money clearing their good names,\textsuperscript{58} while others miss out on significant but fleeting opportunities like employment or home ownership.\textsuperscript{59} Victims could even face criminal charges, as happened to the plaintiff in \textit{Patrick v. Union State Bank}\textsuperscript{60} who was arrested and processed in

\begin{itemize}
\item \textsuperscript{56} Id.
\item \textsuperscript{57} Id.
\item \textsuperscript{58} See Brendan Delany, Comment, \textit{Identity Theft: The Fair Credit Reporting Act And Negligent Enablement Of Impostor Fraud}, 54 \textit{CATH. U. L. REV.} 553, 553 (2005).
\item \textsuperscript{59} For a theoretical example of losing the opportunity to purchase a home, see White, \textit{supra} note 18, at 847. With regard to employment, many companies now require credit checks prehire, as well as for advancement opportunities. See Adam Cohen, \textit{Should Companies Use Credit Checks to Screen Job Applicants?}, \textit{TIME.COM} (Oct. 11, 2011), http://www.time.com/time/nation/article/0,8599,2096608,00.html ("The reliance on credit reports in hiring is becoming widespread. A survey by the Society for Human Resource Management found that 60% of employers do credit checks for at least some positions."). Unlike being rejected for a credit account, where a creditor is required to inform a consumer why he or she was denied credit, a job-seeking identity theft victim may never be made aware of the reason for his or her rejection. See 15 U.S.C. § 1681m(h)(1) (2006).
\item \textsuperscript{60} 681 So. 2d 1364, 1366 ( Ala. 1996).
\end{itemize}
eleven jurisdictions after an identity thief opened a bank account in her name and began passing bad checks. Thus, identity theft victims are subject not only to frustration, stress, and embarrassment, but to real and quantifiable losses. Yet these losses, as we shall see, have not been fully appreciated in many courtrooms across the country.

II. COURTS ARE “UNFRIENDLY TERRITORY” FOR VICTIMS

As discussed, identity theft is an extremely widespread phenomenon in the United States, leaving millions of victims each year to deal with the potentially serious fallout. So it may come as somewhat of a surprise to learn that identity theft victims have been largely unable to obtain redress in civil court, even when the defendant’s culpability is clear and deliberate. In fact, in fourteen states, identity theft victims are not even recognized as victims in a legal sense, making their road to recovery that much more difficult. This is because, historically, an individual whose identity was fraudulently misappropriated was not viewed as the crime’s actual victim. It was the creditor who, at least theoretically, would have to absorb the financial blow of nonpayment when the victim proved the account was fraudulently opened. That antiquated viewpoint misses two key considerations: the deleterious effect of a negative credit account on a victim, discussed in Part I.D above, and that creditors have the option to lend credit more carefully if they so choose, but have not done so believing more stringent measures would hurt business. Yet this theory still resonates in the judiciary, as many victims have been denied recourse. This strange state of

61. See infra notes 105-14 and accompanying text.
63. See Howard, supra note 41, at 1266-67.
64. Id.
65. See id. at 1282.
66. See Arrington, supra note 20, at 373.
affairs led one columnist to remark recently, “[c]ivil court, for now, is unfriendly territory for identity theft victims.”

A. Lack of Recourse Against the Identity Thief

Of all the parties that bear responsibility for an act of identity theft, certainly the identity thief himself is the most directly culpable. Yet, victims can rarely obtain any civil redress from them. Often, this is due to enforcement issues rather than legal ones: identity thieves are hard to find, let alone prosecute, and overburdened law enforcement agencies often lack the resources or the resolve to follow up on the vast majority of identity theft cases. What’s more, official figures do not include many incidents where the victim’s own family misuses his or her identity, an often unreported crime because those victims are either too loyal, too afraid, or too young to prosecute family members just to clear their credit. Lastly, even when identity thieves can be identified and implicated, one can presume they will often have little or no assets for a victim to recover from, and are thus judgment proof.

In the rare event that a thief can be sued directly, victims still face significant legal challenges in obtaining relief from them. Consider, for example, the case of one woman in Nebraska who recently discovered this the hard way. In June 2011, Jaimee Napp sued her identity thief in


68. See Arrington, supra note 20, at 373.

69. Arrests and convictions for identity theft have actually doubled from 2008 to 2009, and prosecutions tripled during the same timeframe. See Javelin Study, supra note 16. However, these numbers are still a small minority of cases. Martha Coakley, the Attorney General for the state of Massachusetts, was herself the victim of identity theft, and she admitted the chances of her “criminal ever being prosecuted are slim to none.” Robert McMillan, Identity Theft Pays, Just Ask Martha Coakley, INFOWORLD (Jan. 22, 2007, 5:02 PM), http://www.infoworld.com/d/security-central/identity-theft-pays-just-ask-martha-coakley-032.

70. See Identity Theft: Is There Another You?: Joint Hearing Before the Subcomm. on Telecomm., Trade, and Consumer Prot. and the Subcomm. on Fin. and Hazardous Materials of the House Comm. on Commerce, 106th Cong. 24 (testimony of Charles A. Albright, Chief Credit Officer, Household International, Inc.) (“In our experience at Household, we find that 50 percent of all incidences of identity theft are committed by another family member.”).

71. See Sullivan, supra note 62.
The defendant, Jackie Brown, was a former coworker who admitted to the accompanying criminal charges of “theft by deception” and served five months in jail. Napp asked the court to award damages for her resulting expenses, including lost time and wages spent repairing her damaged credit, the cost of credit monitoring, and the cost of therapy to treat what her therapist described as post-traumatic stress disorder (“PTSD”) resulting from the incident. According to Napp, she felt as though she was unable to trust her other coworkers after the occurrence and began experiencing paranoia. Judge John Hartigan was perceivably unmoved by Napp’s plight, interrupting her attorney’s closing argument to debate his use of the term identity theft, ruminating that “[i]t’s not like someone took her soul.” He did not similarly interrupt Brown’s attorney, who said that Napp’s claim of PTSD was “a slap in the face to every soldier returning from Iraq” and that she “should ‘move on’ from the incident.” While Nebraska is somewhat unique in being so cold to identity theft victims suing their perpetrators, Judge Hartigan’s insensitivity to fraud victims is not. Indeed, as you will see, a legal indifference to identity theft is a national affliction.

B. Lack of Recourse Against Creditors

With similarly less-than-encouraging results, some identity theft victims have attempted to recover damages against creditors who issue credit accounts to identity thieves. These claims have been traditionally based in common law negligence, sometimes specifically referred to

72. Id.
73. Id.
74. See id.
75. Id.
76. Id.
77. Id.
78. See id. (“There is no law in Nebraska which makes this an easy argument,’ Kuhn said.”). Other states though, such as Alabama, have statutorily defined private rights of action against identity thieves. See, e.g., ALA. CODE § 13A-8-199 (LexisNexis 2005 & Supp. 2007).
as “negligent enablement of imposter fraud.” 79 Other plaintiffs have tried other common law claims such as fraudulent misrepresentation, breach of fiduciary duty, defamation, and breach of contract. 80 The success of these claims varies by state, but they have largely failed to take root. 81 This is despite the fact that creditors, as the final gatekeepers of credit, are uniquely situated to prevent identity theft.

1. Why Hold Creditors Accountable? It seems entirely reasonable to assign the creditor itself a large portion of the blame for an act of identity theft. Unlike CRAs, creditors actually make the fateful decision to extend credit, based on the information obtained from both the applicant and the CRA. 82 Often, as mentioned above, these creditors do not require much consumer information: a name, address, birth date, and social security number, as well as a few questions about your income are all that comprises many credit applications. 83 Of those, only the social security number need be precisely correct: the name and birth date often only need be close to the ones listed on the consumer credit report, while the address and financial information are often wholly fabricated by the identity thief. 84 With more and more data being computerized, and consumer information being required for a growing array of transactions, this information is hardly difficult for an identity thief to obtain. 85 At the same time, the value of credit continues to increase. 86 Thus, it seems grossly counterintuitive for entities as sophisticated as most creditors are to grant access to one of consumer’s most...

80. Arrington, supra note 20, at 372.
81. See id. at 373.
82. See supra note 34 and accompanying text.
83. See supra Part I.C.
84. For example the plaintiff’s creditors in Andrews v. TRW, Inc. opened an account for an imposter where only the plaintiff’s social security number and a bastardized version of her name were based in fact. 225 F.3d 1063, 1065 (9th Cir. 2000), rev’d on other grounds, 534 U.S. 19 (2001).
85. See supra notes 18-24 and accompanying text.
86. See Fed. Trade Comm’n, Getting Credit, supra note 34, at 2.
valuable assets to someone who merely provides—easily misappropriated—information.

And there is a litany of possible protocols that a creditor might adopt that would significantly reduce the probability of granting a credit account to an imposter applicant. Creditors could more scrupulously compare an applicant’s information with his consumer credit report to ensure he is not employing simple identity theft tricks. Creditors could look for the common signs of identity theft, comparing the application to other fraudulent applications. Creditors could call or mail the applicant at the telephone number or address listed on the consumer’s credit report to verify that the application was made by that person. Perhaps the easiest and most effective preventative measure would be for creditors to simply ask for photo identification from applicants; as in my opening example, almost no business nowadays would accept a personal check without proof of identity, yet creditors will routinely give what is essentially a blank check to applicants without such proof.\(^{87}\) Such indifference is unsustainable, but continues in the absence of any meaningful deterrent. Creditors are loath to make consumers go through any more steps than necessary out of a belief that consumer impulsivity benefits their bottom line, and that any voluntary measures would mean potential customers lost to competitors.\(^{88}\) But if an enforceable standard existed requiring all creditors to take certain measures to ensure an applicant’s identity prior to a transaction, it would, at the very least, level the playing field for responsible creditors.

2. Congress (Nearly) Addresses the Problem. Frustratingly enough for victims, Congress actually enacted such a standard called the “Red Flags” rules. In 1970, Congress passed the FCRA, a landmark but ultimately incomplete piece of legislation establishing a baseline of consumer credit rights.\(^{89}\) Congress amended the FCRA via

\(^{87}\) Admittedly, personally checking ID would make the credit process more cumbersome, but it would be up to a jury to decide if such a step would be unduly burdensome. See Andrews, 225 F.3d at 1067. Short of this, technology makes feasible a number of ways to send a copy of an ID, such as scanning and faxing. That is less than ideal, but certainly better than nothing.

\(^{88}\) See Howard, supra note 41, at 1282.

the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), adding, among other things, what could have been a powerful preventative measure called the “Red Flags Guidelines and Regulations.” These rules, subsequently enumerated by regulations that became effective in 2008, require creditors to adopt “reasonable policies and procedures” to identify the warning signs of identity theft and react to those indicators. However, FACTA excluded private enforcement of that standard through the FCRA’s two enumerated causes of action. In effect, Congress created a statutory standard of care, but rendered it toothless by denying a private right of action.

It is plausible, however, that Congress never intended to so limit the Red Flags rules, but simply drafted the amendment poorly. At the time, the FCRA, which FACTA was designed to strengthen, already contained provisions specially authorizing private rights of action for both willful and negligent violations of the Act. FACTA even included a “Rule of Construction” clause articulating Congress’s desire that no provision of the new act would abrogate preexisting liability established by those sections. Nonetheless, Congress obfuscated its meaning by tacking on a subparagraph to the end of an unrelated subsection, exempting the entire section from liability for willful and negligent violations. Due to its placement within a distinct subparagraph, interpreting it as written gives rise to some contradictions and redundancies. Thus, it has been the

91. Id. at 1960-61.
96. This subsection requires users of consumer credit reports to provide notice to a consumer to whom they are offering less favorable terms due to an unfavorable consumer credit report. See 15 U.S.C. § 1681m(h)(1).
98. The limitation on civil actions, if construed literally as pertaining to the entire section, would disallow a private cause of action for violations of the other subsections that conceivably would have been susceptible to private liability.
subject of much debate whether Congress intended to deny a private right of action for the entire section of creditor requirements or merely for that particular subsection.\(^{99}\) Unfortunately for victims, the consensus has been decidedly against a private cause of action.\(^{100}\) Thus, as it stands, the creditor requirements under the FCRA rely solely on administrative enforcement.\(^{101}\)

3. Negligent Enablement of Identity Theft and Common-law Negligence. Left without a clear legislative mandate, victims have sought relief via common law. Basing claims primarily on negligence, plaintiffs have argued that creditors failed to take reasonable measures to protect potential victims from identity thieves, thus enabling identity theft to occur.\(^{102}\) With some notable exceptions,\(^{103}\) however, these claims have not survived.\(^{104}\)

The most notable exception was a 1996 Alabama Supreme Court case, *Patrick v. Union State Bank*,\(^{105}\) and perhaps only because of a particularly sympathetic set of circumstances. Plaintiff Bridgette Patrick had her six-month old baby with her when she was arrested after a pre-FACTA. This would render FACTA’s “Rule of Construction” meaningless. See infra notes 191-94 and accompanying text.


100. *See Perry*, 459 F.3d at 822 (listing a number of cases finding § 1681m(h)(8) to bar private enforcement). *But see Barnette*, 429 F. Supp. 2d at 749.

101. 15 U.S.C. § 1681m(h)(8)(B) (“This section shall be enforced exclusively under section 1681s of this title by the Federal agencies and officials identified in that section.”).


103. *See Wolfe v. MBNA Am. Bank*, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007) (“Because the injury resulting from the negligent issuance of a credit card is foreseeable and preventable, the Court finds that under Tennessee negligence law, Defendant has a duty to verify the authenticity and accuracy of a credit account application before issuing a credit card.”); *Patrick*, 681 So. 2d at 1371 (“[T]he evidence could support a conclusion that [identity theft] was foreseeable and that the bank was in the best position to prevent the fraud, and therefore that the imposition of tort liability could be appropriate.”).

104. *See, e.g.*, Polzer, 682 N.Y.S.2d at 195; Huggins, 585 S.E.2d at 278.

105. *Patrick*, 681 So. 2d at 1364.
The officer had run her license and discovered several warrants for her arrest on the charge of writing "worthless checks." Despite being able to show her handwriting did not match that on the checks, she was held and delivered to police in a nearby county to answer to similar outstanding charges. She spent seventy-two hours there, was exonerated, and was again transferred to another nearby municipality. This grueling process continued in this fashion as she eventually cleared her name in all eleven jurisdictions in which she was wanted; in all, she spent ten days in jail, and several more appearing in court.

The reason for her ordeal was identity theft. An imposter acquired possession of a temporary license issued to Ms. Patrick, used it to open a bank account with the defendant, Union State Bank, and proceeded to make purchases with worthless checks. The bank teller later testified that the imposter supplied no address, the temporary license she presented contained no photo, and that the signature she provided did not even match the one on the license. Nonetheless, the bank allowed the imposter to open the account and issued checks in Ms. Patrick’s name.

Patrick sued Union State Bank for negligence, lost on summary judgment, but convinced the Alabama Supreme Court to reverse. A successful negligence claim generally requires the plaintiff to prove four elements: (1) the defendant owed a duty to exercise a minimum standard of care to the plaintiff, (2) the defendant did not conform to that standard, (3) that failure to conform was the legal cause of harm suffered by plaintiff, and (4) that harm was of

106. Id. at 1366.
107. Id.
108. Id.
109. See id.
110. See id. at n.1.
111. Id.
112. See id.
113. See id. at 1365.
114. See id.
115. See id. at 1372.
the kind that is legally compensable.\textsuperscript{116} Here, the bank argued that Patrick established neither duty nor cause: that “absent a special relationship or special circumstances, a person has no duty to protect another from criminal acts of a third person,”\textsuperscript{117} and that the particular type of harm suffered was not foreseeable.\textsuperscript{118} The court rejected both arguments and reasoned that the bank was not like some innocent bystander but rather a professional entity that in a real way contributed, through its substandard business practices, to the commission of the crime.\textsuperscript{119} The court held that the risk that someone might falsely open an account in another’s name was sufficiently foreseeable for the purposes of establishing both duty and proximate cause, even going so far as to say that incarceration of the innocent party was a probable consequence of such an event.\textsuperscript{120} In any event, the court continued, “[t]he bank undeniably thought that it had a relationship with Ms. Patrick when it opened the account,” thereby assuming a duty.\textsuperscript{121} In so deciding, the court seemingly opened the door for identity theft victims to hold banks accountable when sloppy business practices give imposters access to their credit.

Alas, as quickly as the door was opened, New York’s First Department slammed it shut: only two years after Patrick, it rejected a similar claim for lack of duty. In Polzer v. TRW, Inc.,\textsuperscript{122} a number of identity theft victims sued the Bank of New York and Mobil Oil Credit Corporation for issuing cards in their names to identity thieves.\textsuperscript{123} The plaintiffs invoked a number of theories, including negligent

\textsuperscript{116} Restatement (Second) of Torts § 328A (1965) (“In an action for negligence the plaintiff has the burden of proving (a) facts which give rise to a legal duty on the part of the defendant to conform to the standard of conduct established by law for the protection of the plaintiff, (b) failure of the defendant to conform to the standard of conduct, (c) that such failure is a legal cause of the harm suffered by the plaintiff, and (d) that the plaintiff has in fact suffered harm of a kind legally compensable by damages.”).

\textsuperscript{117} Patrick, 681 So. 2d at 1367.

\textsuperscript{118} See id. at 1371.

\textsuperscript{119} See id. at 1368.

\textsuperscript{120} See id. at 1369.

\textsuperscript{121} See id.


\textsuperscript{123} Id. at 195.
enablement of imposter fraud, simple negligence, negligent infliction of emotional distress, prima facie tort, and violations of the Deceptive Acts and Practices Act. In a cursory opinion, the Appellate Division for the First Department rebuffed them all, and with regard to negligence said:

New York does not recognize a cause of action for “negligent enablement of impostor fraud”, and that plaintiffs otherwise failed to state a cause of action in negligence, because BNY and Mobil had no special relationship either with the impostor who stole the plaintiffs’ credit information and fraudulently obtained credit cards, or with plaintiffs, with whom they stood simply in a creditor/debtor relationship.

The opinion did not elaborate much as to specific facts of the case, nor upon what legal theory it rested its finding, but cited to cases standing for the general common-law precept that there is no “duty to control the conduct of third persons to prevent them from causing injury to others.”

The Polzer court made no mention of the Patrick holding.

Despite its brevity, however, Polzer was influential. In 2003, the Supreme Court of South Carolina cited it in its certified answer to the South Carolina District Court’s blunt inquiry: “Does South Carolina recognize the tort of negligent enablement of imposter fraud?” In that case, Huggins v. Citibank, N.A., despite finding that “it is foreseeable that injury may arise by the negligent issuance of a credit card,” and that such injury “could be prevented if credit card issuers carefully scrutinized credit card applications,” the court held that “[t]he 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.” The court made half-hearted

124. Id.
125. Id. at 196.
126. Id. at 195.
129. Id. at 277.
130. Id.
reference to other potential remedies provided by federal and state statutory regimes, before admitting that “these regulations may not fully compensate victims of identity theft for all of their injury.” As most courts have fallen in line with Polzer, Huggins, and Perry, identity theft victims’ claims against creditors, with rare exception, have not lasted long.

C. Lack of Recourse Against Consumer Reporting Agencies

Nor have claims against CRAs met with any great success. Victims have attempted to hold CRAs accountable for misconduct in both their roles as record keepers and as furnishers of credit reports. As record keepers, CRAs maintain the consumer’s payment history, as reported by creditors. Consumers may challenge erroneous and fraudulent entries in this credit history, though the process is seldom straightforward. But before then, and of much greater concern to our discussion, they furnish consumer credit reports to creditors screening new applicants. To obtain this report, the creditor must provide, along with his or her permission to access the report, some of the applicant’s basic personal information. It is during this phase that the potential for prevention exists.

1. Why Hold CRAs Accountable? Any discussion of identity theft necessitates a discussion of CRAs, or, as they are more commonly known, credit bureaus. This is because identity theft would not be nearly as dire for victims (or perhaps even worthwhile for identity thieves) without the existence of the CRA-issued consumer credit report. Indeed, many of the ill-effects of identity theft discussed in Part I.D—such as denial of credit, disruption of existing credit,
and loss of employment opportunities—occur as a direct result of CRAs issuing a consumer credit report tainted by identity theft. To victims, CRAs become the face of their struggle with identity theft as they work to remove the resulting fraudulent entries from their records. That process is fraught with its own pitfalls for consumers, and consumers must frequently resort to legal actions based in FCRA violations or common law defamation to challenge their reports, with mixed results. Even then, the court has no real power to compel CRAs to remove the bogus entries.

Far from apologetic for these perils, CRAs have even found a way to profit from their specter by selling “credit monitoring services.” For a fee, the CRA will allow a consumer to monitor his or her credit report and receive notices when new activity is logged, with the goal of heading off identity theft. Experian’s version of the service, the misleadingly-named freecreditreport.com, runs television commercials featuring a young bandleader and his misadventures with compromised-credit, suggesting an acute awareness by Experian of the pervasiveness of the problem. Better means for identity theft victims to fix or

137. See Kadet, supra note 134.
138. See Arrington, supra note 20, at 372; White, supra note 18, at 857.
139. See id. (explaining that courts can issue fines, but cannot order the mistake to be corrected).
141. Id.
142. It is misleading because it is not free (only your first seven days of the service is), and its name/URL is suspiciously similar to annualcreditreport.com, the official site established by the FCRA to allow consumers access to their credit reports once per year. See Fed. Trade Comm’n, FTC Consumer Alert: Want a Free Annual Credit Report? The Only Official Website Is AnnualCreditReport.com (2006), http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt156.pdf.
143. In one such commercial, the young man is forced to work at a pirate-themed restaurant because his credit was compromised by “some hacker [who] stole my identity,” thus preventing him from obtaining better employment. See Weezaloo, Funny Commercial from freecreditreport.com, YouTube (Oct. 8, 2007), http://www.youtube.com/watch?v=YWnUmpQhiOw (using freecreditreport.com’s commercial).
remove erroneous credit report entries after the fact are clearly needed, although that worthwhile discussion is somewhat beyond the scope of this Comment. However, these problems suggest that if CRAs are to play any role in identity theft prevention, consumers will need some powerful weapons to compel them to do so.

CRAs are primarily databases of consumer information.144 Pulling a consumer credit report reveals a long forgotten personal history: old addresses, paid-off car loans, and previous employers, all with various levels of accuracy.145 As keepers of such a database, they are uniquely situated to do some preliminary fact-checking when a creditor makes a hard inquiry. As noted in Part II.B.1, many fraudulent credit applications contain gross factual errors—errors that a CRA with its vast database should easily detect. Often, however, the CRA will furnish the report as long as the social security number matches its records.146 The absurdity of such practice was not lost on the Ninth Circuit, which noted that while “people do use nicknames and change addresses . . . how many people misspell their first name? How many people mistake their date of birth?”147 Stranger still, CRAs actually demand much more validation for a consumer to request his own credit report, requiring him correctly provide his name, address, social security number, date of birth, as well as up to four validation questions about his consumer history.148 Some similar common sense procedures at the point of transaction would certainly go far in preventing disastrous results later.

2. Liability Under the FCRA. As it turns out, federal law does place some responsibility on CRAs to verify an applicant’s identity. In Andrews v. TRW Inc., the above-referenced Ninth Circuit case, the court honed in on § 1681b

144. See supra note 35 and accompanying text.
145. See generally ANNUALCREDITREPORT.COM, http://www.annualcreditreport.com (last visited Jan. 26, 2012) (offering options to request a credit report online, by phone, or through the mail).
146. Andrews v. TRW, Inc., 225 F.3d 1063, 1067 (9th Cir. 2000), rev’d on other grounds, 534 U.S. 19 (2001) (“[The credit bureau] let a social security number trump all evidence of dissimilarity between the Plaintiff and the Imposter.”).
147. See id.
of the FCRA, which restricts the circumstances under which a CRA may furnish a consumer credit report. According to that section, a CRA:

may furnish a consumer report under the following circumstances and no other: . . . (3) To a person which it has reason to believe--(A) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer.

The Andrews court focused on the phrase “involving the consumer,” and found that the requirement of reasonable belief applies to this condition, i.e. that the CRA must have “reason to believe” that the credit transaction actually involves the consumer in question. The court rejected the CRA’s argument that lawmakers merely used the term “involv[ing]” in a casual sense, that a transaction merely invokes the consumer’s identity, because “[w]e are reluctant to conclude that Congress meant to harness any consumer to any transaction where any crook chose to use his or her number.”

In that case, a woman’s identity was fraudulently used by a former receptionist at her doctor’s office. Applying for various credit accounts, the imposter combined her own information with Andrews’s last name, birth date, and social security number. She alternatingly used her first name Andrea and a “clumsy misspelling” of victim Andrews’s first name, Adelaide. Andrews sued TRW for furnishing the report to creditors in violation of the FCRA. Her claim was dismissed by the district court, but reinstated by the Ninth Circuit, who held “[i]t is quintessentially a job for a jury to decide whether identity theft has been common enough for it to be reasonable for a credit reporting agency to disclose credit information merely

151. *See Andrews*, 225 F.3d at 1067.
152. *See id.*
153. *Id.* at 1064-65.
154. *Id.* at 1065.
155. *Id.*
because a last name matches a social security number on file.”  In the end, however, Andrews’s claim was quashed by the Supreme Court, who found that the FCRA’s statute of limitations limited claims to within two years of the incident, and thus had expired, in spite of the Ninth Circuit’s insistence that the clock did not start until discovery of the violation.

Although the statute of limitations has since been amended to five years after the incident or two years after discovery, the reversal of Andrews has seemed to hinder its influence. That may be set to change, however, now that the Ninth Circuit has since taken up the issue in Pintos v. Pacific Creditors Association. There, the court held Experian to have violated the FCRA by issuing a credit report on behalf of a consumer, Ms. Pintos, who was not “involved” in the request. Pintos owned a vehicle that was towed for an expired registration, and the towing company “obtained a lien on the vehicle for towing and impound costs.” Pintos did not claim the vehicle or pay the outstanding charges, so the towing company sold it. The sale price did not cover the amount owed, so it asserted a deficiency claim against Pintos and later transferred that claim to PCA, a collection agency. As part of its effort to collect the debt, PCA “sought and obtained” Pintos’s credit report from Experian. Pintos sued PCA and Experian for violating the FCRA by obtaining her credit report without her involvement. Despite the Andrews precedent, the district court granted summary judgment for Experian. Reversing and remanding, the Ninth Circuit revived its holding in Andrews, that to be “involved” in a credit report

---

156. Id. at 1067.
159. Pintos v. Pac. Creditors Ass’n, 605 F.3d 665, 674-75 (9th Cir. 2010).
160. Id. at 675.
161. Id. at 673.
162. Id.
163. Id.
164. Id.
165. Id.
166. Id. at 672.
transaction a consumer must be “a participant.” Without this participation, Experian violated the FCRA by furnishing the report. Adding some fuel to fire, the court further held that § 1681e of the FCRA also requires a CRA to make “a reasonable effort” to verify that a requesting party intends to use the report for a permissible purpose, and if it does not, it may be liable for that requesting party’s FCRA violations. The Supreme Court declined to review the holding, leaving § 1681b a potential tool to attack CRAs who are careless in furnishing consumer credit reports.

3. Negligent Enablement of Identity Theft and CRAs. To the extent that other circuits are not convinced of the Pintos interpretation of §1681b(a), there exist grounds for using common-law negligence against CRAs that furnish credit reports for fraudulent credit applications. Negligence claims have been seldom used in the credit context generally, and have not yet been invoked specifically against CRAs. This is possibly the result of concern over to what extent FCRA preempts related state claims, an area where there has been a good deal of disharmony in judicial interpretation.

It is true that § 1681h(e) and § 1681t(b) do set preemptions on state authority with respect to certain FCRA-related subject matter. Section 1681h(e) grants immunity to CRAs and reporting creditors with respect to the information included in a consumer’s credit report from common-law “defamation, invasion of privacy, or negligence” claims, absent a showing of “malice or willful intent.” Section 1681t(b) enumerates a laundry list of FCRA subject matter upon which states are preempted from...
enacting further requirements.\textsuperscript{175} Some courts have interpreted these two provisions to be complementary, with § 1681h(e) affecting common-law claims and § 1681t(b) referring only to statutory enactments.\textsuperscript{176} In any case, these provisions only apply to certain enumerated subareas, and negligently furnishing a credit report is not among them. The negligence at issue in that instance does not concern the substance of the credit report, as § 1681h(e) relates to. Nor does § 1681t(b) make mention of § 1681b(a), the provision, implicated in \textit{Andrews} and \textit{Pintos}, restricting the issuance of a credit report.\textsuperscript{177} In fact, so long as state law claims are consistent with the requirements of the FCRA, § 1681t(a) specifically preserves their viability.\textsuperscript{178} Thus, the subject of a negligent enablement claim cannot be said to be preempted by the FCRA.

Causation in a CRA negligence claim also becomes a slightly more complicated discussion, as there are two potentially intervening third parties—the identity thief and the creditor.\textsuperscript{179} However, as discussed in Part II.B.3 above, a third party’s negligence or even criminal behavior will not defeat a negligent defendant’s liability if the harm suffered is of the type that made the behavior negligent in the first place.\textsuperscript{180} In the case of CRAs, the possibility of identity theft

\begin{enumerate}
\item[177.] See Pintos v. Pac. Creditors Ass’n, 605 F.3d 665, 672-76 (9th Cir. 2010); Andrews v. TRW Inc., 225 F.3d 1063, 1066-67 (9th Cir. 2000), rev’d on other grounds, 534 U.S. 19 (2001).
\item[178.] 15 U.S.C. § 1681t(a) (2006) (“Except as provided . . . this subchapter does not annul, alter, affect, or exempt any person subject to the provisions of this subchapter from complying with the laws of any State with respect to the collection, distribution, or use of any information on consumers, or for the prevention or mitigation of identity theft, except to the extent that those laws are inconsistent with any provision of this subchapter, and then only to the extent of the inconsistency.”).
\item[179.] See \textsc{Restatement (Second) of Torts} § 441 (1965) (“An intervening force is one which actively operates in producing harm to another after the actor’s negligent act or omission has been committed.”).
\item[180.] See \textsc{Restatement (Second) of Torts} § 449 (1965) (“If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act whether innocent, negligent, intentionally tortious, or criminal does not prevent the actor from being liable for harm caused thereby.”).
\end{enumerate}
is exactly the reason that furnishing credit reports without adequate verification is dangerous. Likewise then, the subsequent culpable actions of creditors and identity thieves should not serve to supersede a CRA’s liability.

Moreover, duty, the stumbling block in many negligent enablement cases, should be even easier to establish for CRA defendants than their creditor counterparts. Aside from the preponderance of general duty considerations of foreseeability and other policy considerations, which will be discussed more in-depth in Part III.B.2 below, the common objection that there exists no “special relationship” between the plaintiff and defendant so as to give rise to a duty to protect is less persuasive in this instance. It is certainly arguable that a “special relationship” could exist between a consumer and a CRA, as there is an existing association between the two, prior to the negligent act, with the former being the subject of the latter’s recordkeeping and the latter being responsible for disclosing the former’s information. That relationship could conceivably give rise to a duty to protect from third-party harm.

III. What Can Be Done?

Administrative enforcement and ex post facto remedial actions only go so far in combating identity theft. As the Court held in Marbury v Madison: “The very essence of civil liberty certainly consists in the right of every individual to claim the protection of the laws, whenever he receives an injury.” But, as we have seen, individuals who become victims of identity theft have largely been unsuccessful in enforcing those protections. Without the threat of private enforcement, the credit industry at-large has not been forthcoming in adopting preventative measures. Congress and the courts must remedy this dynamic; fortunately, this does not require any grand sweeping changes to existing law. In fact, some minor alterations to the FCRA and a fresh look at existing tort concepts would go far in providing redress for victims, and forcing the credit industry to adapt.


A. Legislative Solutions

Congress has taken some important steps in providing consumers baseline credit protection, but is still pulling the punches that could win the fight. Perhaps the simplest and most preferable solution to this situation would be for Congress to amend the FCRA.

First, Congress needs to remove its—perhaps inadvertently placed—limitation on civil liability for violations of the Red Flags rules.\(^{183}\) The standards, as they are now, are painfully vague, requiring creditors to do things like “develop . . . [an] Identity Theft Prevention Program,” and take “reasonable policies and procedures,” to “identify . . . Red Flags” and “[r]espond appropriately.”\(^{184}\) It does finally put the onus on creditors to be proactive, but allowing victims to use the rules to obtain redress would, over time, help define these standards. Once a national standard of reasonable creditor procedures is developed, outlining what procedures are considered reasonable and what responses appropriate, creditors will have no excuse not to adapt, and to adopt preventative measures that may finally turn the tide of identity theft.

Second, although some inroads have been made judicially with regard to CRAs’ liability for furnishing credit reports,\(^ {185}\) a stronger and more specific standard is needed. The statutory phrase “involving the consumer”\(^ {186}\) gives too much possible leeway. The FCRA should specify what basic information the requestor must correctly provide and require some certification that the creditor has made an effort to verify the applicant’s identity.

Third, despite some extension by FACTA, the statute of limitations for an FCRA claim is still insufficient. The FCRA allows, at a maximum, five years from the date of underlying incident to challenge a CRA.\(^ {187}\) Meanwhile, a CRA may lawfully list a delinquent account on a consumer’s

---

\(^{183}\) See supra Part II.B.2.

\(^{184}\) 12 C.F.R. § 41.90(d) (2012).

\(^{185}\) See supra Part II.C.2.


credit report for up to seven years. Thus, the current statute of limitations allows, at a minimum, a two-year gap in which a consumer may have to suffer an erroneous entry with no right to challenge it in court. A modification synchronizing the two timeframes would rescue consumers from being stranded in a procedural no man’s land.

B. Judicial Solutions

Despite Congress’s shortcomings in comprehensively addressing identity theft, and until the courts get on board with holding creditors and CRAs responsible for their careless facilitation of identity theft, preventative measures will be slow to emerge and identity theft will continue to prosper. To that end, the judiciary has many legitimate avenues open to it to expand the credit industry’s liability.

1. Overturn Perry and Allow Private Enforcement of the Red Flags Rules. As discussed briefly in Part II.B.2 above, there is a legitimate question as to whether Congress actually intended to foreclose a private right of action for creditor violations of the Red Flags rules. The provision in question appears as a subparagraph to an amended subsection requiring creditors to provide notice to consumers who are offered less favorable rates due to their credit report. This subparagraph, § 1681m(h)(8)(A), states: “Sections 1681n and 1681o of this title [establishing private rights of action] shall not apply to any failure by any person to comply with this section.” Nonetheless, its placement as a subordinate provision, along with other inconsistencies, begs the question of whether it was meant to apply to the entire section.

The leading case on the subject, Perry v. First National Bank, found the language of the provision unambiguous despite its dubious placement. The Seventh Circuit there admitted that interpreting the tacked-on provisions to apply

---

188. See 15 U.S.C. § 1681c(a)(4) (2006) (noting that “no consumer reporting agency may make any consumer report containing any of the following items of information: . . . (4) Accounts placed for collection or charged to profit and loss which antedate the report by more than seven years”).
190. Id.; see FACTA, § 1681m, 117 Stat. at 1989.
to the entire section would result in some redundancy, but that "redundancy 'does not always produce ambiguity.'" It based its determination largely on the absence of contrary legislative intent, noting "that the legislative history of FACTA is silent on the question of whether Congress intended to preclude private rights of action to enforce the entirety of § 1681m." The court is correct to give important consideration to legislative intent, as it is the primary factor in statutory construction. But the court seems to completely miss the express legislative intent conveyed in the Act's "Rule of Construction" provision, which states:

Nothing in this section, the amendments made by this section, or any other provision of this Act shall be construed to affect any liability under section 616 or 617 of the Fair Credit Reporting Act (15 U.S.C. 1681n, 1681o) that existed on the day before the date of enactment of this Act.

Granted, the Red Flags rules were contained in the same Act, and would not have given rise to an existing liability. However, other subsections that were in existence could potentially be robbed of civil enforceability by interpreting § 1681m(h)(8)(A) to apply to the entire section. For example, § 1681m(a)(3)(A), which requires creditors to notify consumers rejected for credit accounts of their right to obtain a free credit report, existed pre-FACTA and could have given rise to private civil liability if the creditor

---

192. See id. at 821 ("'Section 1681s-2(c),' which was also amended by FACTA, expressly provides that the private remedies sections, 15 U.S.C. §§ 1681n and 1681o, do not apply to one portion of § 1681, namely 15 U.S.C. § 1681m(e), the provision dealing with 'red flagging' of reports affected by identity theft.' According to Perry, 'Congress would not amend 15 U.S.C. § 1681s-2(c) to exempt § 1681m(e) from private remedies if all of § 1681m were already exempt from private remedies by virtue of § 1681m(h)(8).').

193. Id.

194. Id. at 823.

195. See, e.g., Tenn. Valley Auth. v. Hill, 437 U.S. 153, 207 (1978) (Powell, J., dissenting) ("The Court recognizes that the first purpose of statutory construction is to ascertain the intent of the legislature.").


197. Id. at 1960-61.

did not maintain “reasonable procedures to assure compliance” with the section. Thus, to give §1681m(h)(8)(A) the effect of applying to the entire section would directly conflict with the express intent of Congress not to affect existing liability. This violates the primary canon of statutory construction; therefore, that interpretation should be rejected, leaving the Red Flags rules enforceable through private causes of action.

2. Recognize Negligent Enablement of Identity Theft. Finally, courts should begin to recognize and develop a negligence standard of care for the credit industry. For claims against creditors, this embattled approach is perhaps the only attemptable means of redress currently available. Against CRAs, the approach is untested but sound. By allowing these claims to proceed beyond a finding of duty, judges and juries will begin to carve out a standard of care that defines what “reasonable” procedures a purveyor of credit should be expected to take. Only when that standard is identified and enforced will companies start to abide by it, and finally begin preventing identity theft before its destructive effects occur.

a. Establish Duty: Overturning Polzer and Huggins. Courts must recognize the existence of a duty of care between creditors and potential victims. The imposition of a duty is strictly a question of law, and judges frequently struggle with balancing competing policy considerations with existing legal standards. In that regard, it is eminently reasonable for courts to want to limit liability to instances where there is some logical relationship between the tortfeasor and the victim; in fact, it would be terribly unjust to hold otherwise. But the majority view that there is no relationship between an identity theft victim and the creditor who opened the account in question is untenable. A relationship such that would give rise to a duty of care can be reached through a variety of means; to imply that some sort of preexisting, on-going relationship is necessary for an actor to be compelled to take reasonable care not to harm a readily identifiable party is an unwarranted hurdle to justice. Privity as a precursor to duty has, post—MacPherson v. Buick Motor Company, long been discredited.


200. MacPherson v. Buick Motor Co., 111 N.E. 1050, 1053 (N.Y. 1916) (“We have put aside the notion that the duty to safeguard life and limb, when the
Yet these cases rely heavily on the antiquated precept that a negligent party may not be held liable for the criminal acts of another absent some “special relationship” to the plaintiff.\(^{201}\) significantly over the years, as negligent defendants have long been held liable for third-party acts so long as the harm was of the type that made the misfeasance negligent in the first place.\(^{202}\) To the extent that it remains a viable defense, it is usually reserved for intentional physical harm caused by third parties.\(^{203}\) At any rate, as the Patrick court pointed out, the creditor in an identity theft case “undeniably thought that it had a relationship with [the victim] when it opened the account.”\(^{204}\) Thus, by the bare act of opening an account in someone’s name, the creditor arguably undertakes a relationship with that person. At the very least, it should be aware that it will be affecting that person in a profound way. Similar to claims for defamation or invasion of privacy, there is no tangible interaction between the defendant and the victim, but there is an affirmative act that invokes a specific innocent party. Therefore it is reasonable to necessitate that some care be taken to prevent that party from being harmed.

Hence, duty here should be determined by more general duty principles; adjudged by which, a strong case for the imposition of duty can be made. In fact, the sheer foreseeability of probable harm and the knowledge of the specific party who stands to be affected provides a clear basis for establishing a duty. Foreseeability, in most jurisdictions, is the most important factor in determining the existence of a duty.\(^{205}\) Foreseeability is evaluated from

---


\(^{202}\) See Restatement (Second) of Torts § 449, supra note 180.

\(^{203}\) Patrick v. Union State Bank, 681 So. 2d 1364, 1367 (Ala. 1996) (“The cases applying the rule address the question whether a defendant owes a duty to protect the plaintiff from violent physical criminal acts of a third person. In fact, the rule has been stated as being that 'one has no duty to protect another from criminal attack by a third party.'”).

\(^{204}\) Id. at 1369.

\(^{205}\) Benjamin C. Zipursky, Foreseeability in Breach, Duty, and Proximate Cause, 44 Wake Forest L. Rev. 1247, 1258 (2009) (“Almost every jurisdiction
the perspective of a reasonably prudent person in similar circumstances. In the case of identity theft, it is practically a foregone conclusion: with millions of new victims affected each year, the risk of identity theft is nearly an inevitable consequence of negligent credit practices. Nearly any person off the street knows the substantial threat of identity theft, and thus a person whose business is credit would have to have his proverbial head in the sand not to be keenly aware of the looming risk of fraud.

Yet mere foreseeability does not give rise to a duty. Duty, as a judicial policy decision, must take into account a myriad of more subjective public policy considerations, such as “the relationship of the parties, the nature of the attendant risk, the opportunity and ability to exercise care, and the public interest in the proposed solution.” Here the relationship is that between a sophisticated defendant and a practically helpless plaintiff: the former actively engaged in the business of extending credit, and well aware of its power and appeal to criminals, and the latter who—in most cases—would have no reason to suspect that he is being victimized and has few means to protect himself from it even if he did. The opportunity to take steps to prevent the harm is available only to the defendant, and indeed, he is the last line of defense to this harm. The risk of fraud is inherent in the business of credit, as it is one of essentially selling money, and indeed one of the primary reasons creditors run credit checks on its applicants is to screen out those who have records of being dishonest or criminal. To place the responsibility of verifying an applicant’s identity on a creditor would not be an undue burden or too broad a does treat foreseeability as a significant factor (and frequently the most significant factor) in analyzing whether the duty element is met in a negligence claim.

206. See Javelin Study, supra note 16.
208. See Fed. Trade Comm’n, Credit, ATM, and Debit Cards, supra note 22, at 2-3.
liability to impose, but rather an intrinsically reasonable one in considering the circumstances. Thus, judges should and do recognize a duty of care.

b. Standard of Care, Legal Causation, and Damages. Once the judicially-determined barrier of duty is dismantled, the remainder of a negligence claim is easily palatable. Breach, or standard of care, would rightly be a jury question, and should take into account Learned Hand’s principles, i.e., determining what relatively unburdensome measures a creditor could take to prevent a very probable harm.211 Certainly the Red Flags rules should also come into play as an effective standard,212 if not as a per se presumption of negligence, at least as evidence that it would not take any additional effort for creditors to undertake the measures that they are already legally obligated to assume. Of course, creditors could not, and should not, be liable for every case of identity theft, but only those cases where the creditors did not adhere to a minimum standard of preventative measures. But therein lies the most important reason why these claims need to be encouraged—to develop this minimum standard for creditors to follow.

The remaining factors are relatively straightforward. A creditor’s negligent issuance of a credit account would be a very substantial factor in any consummated act of identity theft and thus, its legal cause.213 Proximate cause, mainly defined by foreseeability, is also straightforward, as the type of harm suffered is exactly the type that one might expect from such negligence.214 That harm, of course, takes

211. See United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) (suggesting that negligence may be inferred when the burden of avoiding the harm is less than the cost of the harm multiplied by its probability of occurrence, and that the burden is not undertaken).

212. See Kevin D. Lyles, Red Flag Rules Require Companies to Take Identity Theft Seriously, JONES DAY (Nov. 2008), http://www.jonesday.com/red-flag-rules-require-companies-to-take-identity-theft-seriously-11-12-2008/ (“In any event, it is likely that, over time, the Red Flag Rules will become a de facto standard of care applied to determine whether a company has negligently allowed a customer’s identity to be stolen.”).

213. See RESTATEMENT (SECOND) OF TORTS § 431 (1965) (“The actor’s negligent conduct is a legal cause of harm to another if (a) his conduct is a substantial factor in bringing about the harm, and (b) there is no rule of law relieving the actor from liability because of the manner in which his negligence has resulted in the harm.”).

214. See RESTATEMENT (SECOND) OF TORTS § 449, supra note 180.
the form of the sometimes devastating damages discussed in Part I.D of this Comment.

These non-duty issues are primarily questions of fact, and therefore the average jury—who will be almost statistically certain to have had some connection with identity theft—would be deciding whether the credit industry is doing enough to prevent fraud. The jury’s answer is likely to change the way the credit industry operates forever, providing, at long last, a line of defense against identity theft.

CONCLUSION

Despite increased awareness, identity theft has continued to thrive. Once victimized, an individual can spend years trying to clear his or her name, meanwhile suffering from the stigma of bad credit that may include denial of services, loans, and employment, as well as humiliation and even arrest. Victims are left with virtually no means of obtaining remedy for these sometimes substantial losses, even against those who are responsible for the fraud’s occurrence. Likewise, while existing law provides some measure of assistance to fraud victims seeking to clean up their credit after the fact, it does little to prevent future occurrences. Quite remarkably, credit-granting companies require very little proof of identity to open new accounts. Even in the face of surging identity theft rates, a social security number and most of a name are often all that is required to obtain a credit card or turn on utilities. Certainly this lackadaisical attitude toward identity theft is partially responsible for identity theft’s continued prominence. These inadequacies in prevention and redress could be addressed by increasing the accountability on credit-granting institutions. No major legal overhaul is necessary to accomplish this; merely allowing private enforcement of existing federal and common law standards would suffice in promoting some common-sense reforms. Nevertheless, until Congress and the courts get serious about enforcing identity theft prevention, the fight against identity theft will continue to be a losing battle.