

2002

## Comment: Identity Theft: Victim "Cry Out" for Reform

Erin M. Shoudt

*American University Washington College of Law*

Follow this and additional works at: <http://digitalcommons.wcl.american.edu/aulr>



Part of the [Law Commons](#)

---

### Recommended Citation

Shoudt, Erin M. "Comment: Identity Theft: Victim "Cry Out" for Reform." *American University Law Review* 52, no.1 (2002):339-392.

This Comment is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Law Review by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact [fbrown@wcl.american.edu](mailto:fbrown@wcl.american.edu).

---

Comment: Identity Theft: Victim "Cry Out" for Reform

# IDENTITY THEFT: VICTIMS “CRY OUT” FOR REFORM

ERIN M. SHOUDT\*

## TABLE OF CONTENTS

Introduction.....	340
I. The Nature of Identity Theft.....	342
II. The Supreme Court Addresses Identity Theft.....	345
A. Facts.....	346
B. The Lower Courts’ Analyses.....	349
C. The Supreme Court Opinion .....	353
III. The Legal System and the Credit Industry Create Burdens on Identity Theft Victims .....	356
A. Burdens Imposed Through the Legal System .....	357
B. Inefficient Procedures in the Credit Reporting Industry Impose Additional Burdens .....	365
IV. The FTC Response to Identity Theft.....	369
A. The FTC Initiatives under the Identity Theft and Assumption Deterrence Act.....	371
1. The identity theft hotline .....	372
2. The identity theft clearinghouse.....	373
3. Consumer education .....	374
B. The FTC Successes .....	375
C. The FTC Prevention Efforts.....	375
V. Possible Agency and Legislative Proposals.....	382
A. Voluntary Initiatives .....	382
B. Legislative Proposals.....	385
1. Legislation to hold the credit industry accountable ...	386
2. Legislation to amend the Fair Credit Reporting Act ..	389
Conclusion .....	392

---

\* J.D. Candidate, May 2003, *American University, Washington College of Law*; B.A., 1998 *Colgate University*. I would like to thank Robert Vaughn, Jill Savedoff, and Kristina Hickerson for their advice, guidance, and editing suggestions. Special thanks to my family and friends for their constant support and encouragement.

## INTRODUCTION

On February 23, 2001, Abraham Abdallah, a busboy from Brooklyn, New York, was arrested for using the Internet at public libraries to steal the identities of more than 200 of the wealthiest business moguls in the United States, including Steven Spielberg, Oprah Winfrey and Ted Turner.<sup>1</sup> After acquiring the celebrities' social security numbers, credit reports, account numbers and addresses, Abdallah accessed their credit card and investment accounts and made an estimated \$100 million worth of purchases on the Internet.<sup>2</sup> In April 2001, a California court sentenced a man to 200 years to life in prison for using the identity of Tiger Woods to buy \$17,000 worth of goods, including a television and a luxury car.<sup>3</sup> On June 5, 2001, after a request from the Governor, the Florida Supreme Court issued an order to impanel a grand jury to investigate the growing problem of identity theft.<sup>4</sup> Currently, numerous legislative bills addressing the privacy of personal data are pending in the U.S. Congress.<sup>5</sup> Significantly, the U.S. Supreme Court decided its first case involving identity theft in November 2001.<sup>6</sup>

These legislative and judicial responses reflect the growing national concern over privacy of personal information and identity theft.<sup>7</sup>

---

1. See Murray Weiss, *How NYPD Cracked the Ultimate Cyberfraud-B'klyn Busboy Busted in Theft of 200+ Tycoon IDs*, N.Y. POST, Mar. 20, 2001, at 4 (reporting that Abdallah used the Internet, cellular phones, and voice mailboxes to steal identities of the wealthiest Americans listed in Forbes 400).

2. See *id.* (explaining that Abdallah's cybercrime has been considered one of the largest identity theft cases in Internet history); see also *Protecting Privacy and Preventing Misuse of Social Security Numbers: Hearing Before the House Comm. on Ways and Means, Subcomm. on Soc. Sec.*, 107th Cong. 60 (2001) [hereinafter *Ways and Means Hearings*] (statement of Michael Fabozzi, Detective, New York City Police Department) (recounting Abdallah's strategy for stealing identities).

3. See *Someone Else Loses to Tiger Woods*, CARDFAX, Apr. 30, 2001 (explaining that Anthony Lemar Taylor, who had been convicted of 20 misdemeanors, was sentenced under California's three strikes law), available at 2001 WL 8724954, \*1.

4. See *Grand Jury Seated to Study Identity Theft*, TAMPA TRIB., June 5, 2001, at 2 (explaining that eighteen jurors will be selected to investigate identity theft).

5. See, e.g., Social Security Number Privacy and Identity Theft Prevention Act of 2001, H.R. 2036, 107th Cong. (2001) (amending the Social Security Act to enhance privacy protections and to prevent fraudulent misuse of social security account numbers); Identity Theft Prevention Act of 2001, S. 1399, 107th Cong. (2001) (amending the Fair Credit Reporting Act to develop procedural guidelines for credit reporting agencies' handling of discrepancies in a consumer's account).

6. See *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (holding that a general discovery rule does not apply to toll the statute of limitations for suits under the Fair Credit Reporting Act); see also David G. Savage, *Court Set for New Term and Novel Issues*, L.A. TIMES, Sept. 30, 2001, at A37 (explaining that the Supreme Court will examine the issue of whether the statute of limitations begins when identity theft is committed or when it is discovered).

7. See 147 CONG. REC. E988 (daily ed. May 25, 2001) (statement of Hon. E. Clay Shaw, Jr. (Fla.)) (referring to a Wall Street Journal article in which respondents ranked privacy as their primary concern above war and environmental disasters).

Identity theft is defined as a crime where “an individual appropriates another’s name, address, social security number, or other identifying information to commit fraud.”<sup>8</sup> Recently, the U.S. Attorney’s Office recognized identity theft as “the crime of the new millennium.”<sup>9</sup> Consumer interest groups have called identity theft “one of the nation’s fastest growing white-collar crimes.”<sup>10</sup> Identity theft has become “a national crisis,”<sup>11</sup> as personal information is becoming more accessible, and as the above cases illustrate, criminals are becoming more computer literate and technologically savvy.<sup>12</sup>

Identity theft is unique because consumers do not know they have become victims of identity theft until an application for employment, a loan, or a mortgage is denied because an imposter has destroyed their credit reports or has established criminal records in their names.<sup>13</sup> Approximately 500,000 to 700,000 people become victims of identity theft annually.<sup>14</sup> The burden on victims of identity theft is significant as they face the arduous tasks of reestablishing their credit ratings and their reputations.<sup>15</sup>

---

8. *The Identity Theft and Assumption Deterrence Act: Hearing on S.J. Res. 512 Before the Senate Comm. on the Judiciary, Subcomm. on Tech., Terrorism, and Gov’t Info.*, 105th Cong. 17 (1998) [hereinafter *May 20, 1998 Hearings*] (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, Federal Trade Commission (“FTC”)) (presenting the FTC’s views on identity theft).

9. Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, U.S. ATT’YS’ USA BULL., Mar. 2001, 1, available at [http://www.usdoj.gov:80/criminal/cybercrime/usamarch2001\\_3.htm](http://www.usdoj.gov:80/criminal/cybercrime/usamarch2001_3.htm) (last visited May 29, 2001).

10. *Ways and Means Hearings*, *supra* note 2, at 118 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group).

11. *Id.* at 16 (statement of Hon. James G. Huse, Jr., Inspector General, Social Security Administration); *see also* 147 CONG. REC. E989 (daily ed. May 25, 2001) (statement of Hon. E. Clay Shaw, Jr.) (reporting that allegations of fraudulent use of social security numbers increased nearly fifty percent between 1999-2000).

12. *See May 20, 1998 Hearings*, *supra* note 8, at 11 (statement of James Bauer, Deputy Assistant Director, U.S. Secret Service) (stating that the Internet has led to an increase in identity fraud); *see also* Robert O’Harrow, Jr., *Identity Thieves Thrive in Information Age: Rise of Online Data Brokers Makes Criminal Impersonation Easier*, WASH. POST, May 31, 2001, at A1 (reporting that identity thieves are now using personal information from commercial online data brokers, which collect and sell the data for a fee).

13. *See May 20, 1998 Hearings*, *supra* note 8, at 19 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC) (stating that the harm resulting from identity theft “may not be readily apparent or easily quantifiable”).

14. 147 CONG. REC. S6129 (daily ed. June 12, 2001) (statement of Sen. Jim Bunning); *see* 147 CONG. REC. S4591 (daily ed. May 9, 2001) (statement of Sen. Dianne Feinstein) (stating that the FBI estimates that 350,000 cases of identity theft occur each year); O’Harrow, *supra* note 12, at A9 (citing that the Federal Office of the Comptroller of the Currency estimated 500,000 victims of identity theft per year).

15. *See May 20, 1998 Hearings*, *supra* note 8, at 20 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC) (explaining the time-consuming process of clearing a fraudulent credit report).

This Comment will explore the relationship between the victims of identity theft and the credit reporting agencies.<sup>16</sup> It will argue that both recent interpretation of the statutory language of the Fair Credit Reporting Act (“FCRA”) and credit reporting agencies’ inefficient procedures make a victim’s recovery process almost impossible.<sup>17</sup> Part I will describe the two main types of identity theft. Part II will examine the U.S. Supreme Court’s recent decision in *TRW Inc. v. Andrews*,<sup>18</sup> which held that the statute of limitations for an action against a credit reporting agency begins at the time of the initial violation of the FCRA, rather than when the victim discovers the injury.<sup>19</sup> Part III will address the statutory and procedural barriers that hinder rapid remediation for the identity theft victim. It will further assert that the procedural inefficiencies created by the credit industry, as well as the statutory burden the Supreme Court condoned in its recent decision, only make a victim’s recovery process more difficult.

Part IV will survey federal agency responses to the identity theft crisis. Specifically, this Part will examine the mechanisms the Federal Trade Commission (“FTC”) has established to fulfill its obligations under the Identity Theft and Assumption Deterrence Act and the strides the FTC program has made in educating consumers, reducing the burdens on victims, and preventing identity theft. Finally, Part V will address the voluntary initiatives and legislative proposals that could make a real impact on the identity theft victim’s recovery process. In light of the spreading identity theft epidemic, it will conclude that Congress should look with increased vigor at the role of the credit reporting agencies in the identity theft crisis.

## I. THE NATURE OF IDENTITY THEFT

Identity theft affects victims in two principle realms—the financial realm and the criminal realm.<sup>20</sup> The misappropriation of another’s

---

16. See 15 U.S.C. § 1681a(f) (2000) (defining a consumer reporting agency as a person who participates 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”).

17. See Erika Morphy, *New Privacy Laws, Please, But Not for E-Tailers*, ECOMMERCE TIMES, Oct. 18, 2001 (explaining that the statute of limitations issue is only one barrier to consumers who want to maintain good credit, the other issue being the burden on the victim of identity theft to clear an erroneous credit report), available at <http://www.ecommercetimes.com/perl/story/14244.html> (last visited Aug. 1, 2002).

18. 534 U.S. 19 (2001).

19. See *id.* at 28 (imposing a substantial burden on victims of identity theft and holding that the language of the FCRA precludes implication of a discovery rule).

20. See *Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the*

personal information can ruin one's financial history and can create a criminal record in the victim's name.<sup>21</sup> Whether an imposter obtains another's personal identification information by "low tech"<sup>22</sup> methods, more sophisticated means,<sup>23</sup> or even from the Internet,<sup>24</sup> the effect on the victim's credit and reputation can be devastating.<sup>25</sup>

The most common misappropriation of another's personal identifiers is financial identity theft, which can occur in many forms.<sup>26</sup> In an "account takeover," the criminal accesses the victim's existing credit card account to make unauthorized charges.<sup>27</sup> The thief often

---

*Senate Comm. on the Judiciary, Subcomm. on Tech., Terrorism, and Gov't Info.*, 106th Cong. 32 (2000) [hereinafter *July 12, 2000 Hearings*] (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (explaining that identity theft can be financial or criminal in nature).

21. *Id.*; see generally Brandon McKelvey, Comment, *Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft*, 34 U.C. DAVIS L. REV. 1077, 1082-88 (2001) (providing an overview of the various types of identity theft and its impact on consumers).

22. See *Identity Theft: Is There Another You?: Joint Hearing Before the House Comm. on Commerce, Subcomm. on Telecom., Trade, and Consumer Prot. and Subcomm. on Fin. and Hazardous Materials*, 106th Cong. 18 (1999) [hereinafter *April 22, 1999 Hearings*] (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (discussing low tech methods of identity theft, such as rummaging through trash for bank statements or discarded credit card offers); see also *July 12, 2000 Hearings, supra* note 20, at 33 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (explaining that "the old fashioned way" of obtaining personal information is to steal a purse or wallet and either personally use the information or provide the contents to a crime ring).

23. See *July 12, 2000 Hearings, supra* note 20, at 33 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (describing a method called "the inside job" in which an employee who has access to client information steals their identities); see also *April 22, 1999 Hearings, supra* note 22, at 19 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (defining "skimming" as the act of copying information on a magnetic strip of an ATM or credit card and re-encoding it onto another card, transforming a blank card into one identical to that of the victim).

24. See *ID Theft: When Bad Things Happen to your Good Name: Hearing Before the Senate Comm. on the Judiciary, Subcomm. on Tech., Terrorism, and Gov't Info.*, 106th Cong. 32 (2000) [hereinafter *March 7, 2000 Hearings*] (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (stating that "[t]he Internet has dramatically altered the potential impact of identity theft"); see also *id.* at 23-24 (statement of Gregory Regan, Special Agent in Charge, Financial Crimes Division, U.S. Secret Service) (explaining that the Internet increases identity theft because it creates a "faceless society" and "provides the anonymity that criminals desire").

25. See, e.g., *July 12, 2000 Hearings, supra* note 20, at 24 (statement of Michelle Brown, victim) (describing the trauma she experienced with financial and criminal identity theft); see also 147 CONG. REC. E1030 (daily ed. June 6, 2001) (statement of Hon. Darlene Hooley) (explaining a case in which someone stole the identity of a child who died and was claiming him as a dependent on their income tax return).

26. See *April 22, 1999 Hearings, supra* note 22, at 18 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (stating that "[i]dentity theft almost always involves a financial services institution," but may take on a variety of forms such as taking out loans, writing fraudulent checks, or opening a bank account in another's name).

27. See *id.* (describing one of the many types of identity theft); see also U.S. GOV'T ACCT. OFFICE, No. GAO/GGD-98-100BR, IDENTITY FRAUD: INFORMATION ON

reports a change of address to the credit card company to avoid discovery by the victim.<sup>28</sup> In “true person fraud,” the criminal assumes another’s complete identity and applies for new credit in the victim’s name.<sup>29</sup> When credit card bills are not paid, the debt is reported on the victim’s credit report.<sup>30</sup> The victim is usually not aware of the theft until, for example, a loan application is denied due to a poor credit history.<sup>31</sup>

In March 2001, the FTC reported that opening new accounts and making unauthorized charges to existing accounts on credit cards or utilities were the most common identity theft cases.<sup>32</sup> The FTC also reported that approximately fifty percent of victims experience multiple types of identity theft,<sup>33</sup> including the criminal obtaining loans and mortgages, transferring money from bank accounts, and writing fraudulent checks using the victim’s identity.<sup>34</sup>

---

PREVALENCE, COST, AND INTERNET IMPACT IS LIMITED 18 (May 1998) [hereinafter GAO REPORT] (identifying three types of financial identity theft addressed in different sections of the U.S. Code).

28. See *April 22, 1999 Hearings*, *supra* note 22, at 18 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (describing the strategy used by the thief to execute an account takeover).

29. See GAO REPORT, *supra* note 27, at 18 (defining true person fraud and distinguishing it from other forms of fraud); see also *July 12, 2000 Hearings*, *supra* note 20, at 34 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (explaining that identity thieves can also gain employment in the victim’s name).

30. See *March 7, 2000 Hearings*, *supra* note 24, at 32 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining that consumers credit history is usually scarred).

31. See *id.* (stating that consumers may be denied mortgages, loans, new bank accounts, and even employment due to the identity thief’s activities).

32. See FEDERAL TRADE COMMISSION, IDENTITY THEFT COMPLAINT DATA: FIGURES AND TRENDS ON IDENTITY THEFT NOVEMBER 1999 THROUGH MARCH 2001 2 (2001) [hereinafter MARCH 2001 DATA] (stating forty-seven percent of victims who contacted the FTC reported credit card fraud and twenty-two percent reported fraudulent utility service).

33. See *id.* at 3 (reporting that half of the victims experience a combination of identity theft, whether it be both credit card fraud and bank fraud, or the creation of new utility accounts and personal loans).

34. See *id.* at 2 (showing that fifteen percent of victims reported that identity thieves wrote fraudulent checks, made unauthorized bank withdrawals, and established new bank accounts, and eight percent reported that thieves had obtained fraudulent loans); see also *May 20, 1998 Hearings*, *supra* note 8, at 19 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC) (explaining that criminals usually seek out consumers with high incomes and good credit).

Criminal identity theft, termed “the worst case scenario,”<sup>35</sup> affects approximately eleven percent of consumer victims.<sup>36</sup> In criminal identity theft, the criminal gives the victim’s personal identifying information to a law enforcement officer upon arrest or issuance of a citation.<sup>37</sup> When the imposter does not appear in court, a warrant for arrest will be issued in the victim’s name.<sup>38</sup> The victim often will find out about the crime committed in his or her name only when he or she commits a traffic violation and a law enforcement officer runs a background check.<sup>39</sup> A victim may also become aware of the identity theft when denied employment after the employer conducts a background investigation revealing the imposter’s criminal conduct.<sup>40</sup>

## II. THE SUPREME COURT ADDRESSES IDENTITY THEFT

The Supreme Court recently heard the story of Adelaide Andrews, a classic case of financial identity theft.<sup>41</sup> The Supreme Court’s 9-0 decision has highlighted one obstacle that a victim faces in recovering from identity theft.<sup>42</sup> In Andrews’ case, the Court held

---

35. *July 12, 2000 Hearings, supra* note 20, at 34 (statement of Beth Givens, Director, Privacy Rights Clearinghouse); see PRIVACY RIGHTS CLEARINGHOUSE, FACT SHEET 17(G), CRIMINAL IDENTITY THEFT WHAT TO DO IF IT HAPPENS TO YOU [hereinafter FACT SHEET 17(G)] (defining criminal identity theft and explaining what to do if you are a victim), at [www.privacyrights.org/fs/fs17g-CrimIdTheft.htm](http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm) (last visited Jan. 28, 2002).

36. See FTC, IDENTITY THEFT VICTIM ASSISTANCE WORKSHOP 16 (Oct. 23, 2000) [hereinafter IDENTITY THEFT WORKSHOP] (remarks of Joanna Crane, Attorney, Division of Planning and Information, FTC) (explaining prevalence of criminal identity theft).

37. See *July 12, 2000 Hearings, supra* note 20, at 24 (statement of Michelle Brown, victim) (recounting her experience when she received a prison sentence because an imposter gave her information to the DEA and a federal judge when the imposter was caught trafficking marijuana); see also FACT SHEET 17(G), *supra* note 35 (stating that criminal identity theft can happen through use of a counterfeit driver’s license containing another’s information).

38. See FACT SHEET 17(G), *supra* note 35 (outlining the techniques criminal identity thieves use); see also *July 12, 2000 Hearings, supra* note 20, at 34 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (citing a case in which a victim was returning to the United States from Mexico and was put in jail for ten days when a search revealed he was wanted for a crime, which in fact was perpetrated by an imposter).

39. See FACT SHEET 17(G), *supra* note 35 (explaining that the victim may be arrested and taken to jail because of an outstanding warrant in his or her name).

40. See *id.* (noting that an employer is legally obligated to inform the victim of the reason for rejection, which puts the victim on alert).

41. See *TRW, Inc. v. Andrews*, 534 U.S. 19, 23 (2001) (reporting that Adelaide Andrews’ personal information was stolen by a receptionist at her radiologist’s office and was used to open various credit accounts).

42. See *id.* at 21 (stating that seven justices joined the majority opinion and two justices filed an opinion concurring in the judgment); see also *Identity Theft: Special Report*, CONSUMER REPS., Sept. 1997, at 10 (describing that suing credit reporting agencies for improper disclosures is a new avenue of recourse for identity theft victims).

that the statute of limitations for a suit against a credit reporting agency for improper disclosures begins at the time of the initial violation of the FCRA, not when the victim discovers that an improper disclosure occurred.<sup>43</sup> As a result of this decision, victims will lose their opportunity to file a claim against a credit reporting agency for improper disclosures if they learn of the occurrence of a violation at any time after the two-year statute of limitations has expired.<sup>44</sup>

#### A. Facts

Adelaide Andrews' ordeal with identity theft began at a doctor's visit on June 17, 1993.<sup>45</sup> At that visit, Andrews completed a Patient Information form, which included, among other standard information, her name, social security number, home address, driver's license number, and date of birth.<sup>46</sup> The receptionist, Andrea Andrews (the "Imposter"), copied Adelaide Andrews' personal information and subsequently relocated to Las Vegas, Nevada.<sup>47</sup> After moving to Las Vegas, the Imposter used Andrews' personal information to rent an apartment and to establish telephone and electric service.<sup>48</sup>

The Imposter then attempted to obtain services from five creditors,<sup>49</sup> which subscribed to two different credit reporting agencies.<sup>50</sup> On October 22, 1994, the Imposter applied for a credit account at Dillard's department store, using her own name, her Las Vegas address, and Andrews' social security number on the

---

43. See *TRW*, 534 U.S. at 22-23 (holding that a discovery rule, in which the statute of limitations would begin to run at the time of the plaintiff's discovery of the violation, does not apply to cases under the FCRA).

44. See *Borrowers Beware*, N.J. LAW.: WKLY. NEWSPAPER, Dec. 3, 2001, at 6 (reporting that a consumer, who does not request a credit report every two years, risks losing the opportunity to sue the credit reporting agency for damages from improper disclosures).

45. *Andrews v. Trans Union Corp.*, 7 F. Supp. 2d 1056, 1063 (C.D. Cal. 1998), *aff'd in part, rev'd in part sub nom. Andrews v. TRW, Inc.*, 225 F.3d 1063 (9th Cir. 2000) *rev'd* 534 U.S. 19 (2001).

46. *Id.*

47. See *id.* (recounting the Imposter's technique).

48. See *id.* (explaining how the Imposter used the name "Adelaide (Andrea) Andrews" on her apartment lease application and noting that credit reports were not requested for the Imposter's apartment lease, telephone, and utility service applications).

49. See *id.* (indicating that the basis of Andrews' suit against the credit reporting agency arises from these five attempts by the Imposter to secure lines of credit using Andrews' personal information).

50. See *id.* at 1062 (explaining that when a consumer applies for credit, the credit grantor will obtain reports from a credit reporting agency to assess the customer's credit and to determine whether the grantor should approve the application for credit).

application.<sup>51</sup> Dillard's obtained its credit reports from Trans Union Corporation, the defendant in Andrews' original action.<sup>52</sup> When the Imposter's first initial, last name, and social security number matched those on the credit report file, Trans Union provided the credit report to Dillard's.<sup>53</sup> Dillard's then approved the Imposter's application for a line of credit and the account later became delinquent.<sup>54</sup>

TRW Inc. ("TRW"),<sup>55</sup> the credit reporting agency implicated in Andrews' case in the Supreme Court, was the agency used by four other creditors to whom the Imposter applied for a line of credit.<sup>56</sup> On July 25, 1994, the Imposter used Andrews' birth date and social security number on an application to First Consumers National Bank ("FCNB").<sup>57</sup> On September 27, 1994, the Imposter applied for a credit account from Prime Cable of Las Vegas, for which she used Andrews' social security number.<sup>58</sup> On October 28, 1994, the Imposter submitted an application to Express Department Stores, using her own identifying information but misappropriating Andrews' social security number.<sup>59</sup> Finally, in January 1995, the Imposter applied for credit from a retail lender, using her own identity but employing Andrews' social security number and a misspelling of Andrews' first name.<sup>60</sup>

---

51. *Id.*

52. *Id.*

53. *See id.* (noting that the Trans Union database showed one file on Andrea Andrews, the Imposter, and two files on Adelaide Andrews, the plaintiff). The Imposter's file listed the Las Vegas address, but no social security number, and Andrews' two files showed her Santa Monica address and a previous address in Texas. *Id.* Although differences in the files existed, Trans Union provided all three reports to Dillard's because the social security number, last name, and first initial matched. *Id.* Trans Union, however, did include a "Trans Alert" warning to notify Dillard's of the differing addresses. *Id.*

54. *See id.* (citing one instance of harm caused by the Imposter).

55. *See* Experian, *Ask Max* (Apr. 23, 1997) (noting that TRW, Inc. had formerly been one of three national credit bureaus, but Experian Information Solutions, Inc. later assumed control over its business), available at <http://www.experian.com/corporate/max/max042397.html> (last visited Aug. 5, 2002).

56. *See* *Andrews v. Trans Union Corp.*, 7 F. Supp. 2d 1056, 1063 (C.D. Cal. 1998) (stating that TRW, Inc. provided credit reports in the four other circumstances in which the Imposter attempted to obtain services and credit).

57. *Id.*; *see* *Andrews v. TRW, Inc.*, 225 F.3d 1063, 1065 (9th Cir. 2000) (providing details of the Imposter's attempt to gain credit from FCNB, for which she used her own name, but Adelaide's date of birth and social security number).

58. *See* Respondent's Brief at 5, *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (No. 00-1045) (reciting yet another attempt by the Imposter to use Andrews' identity to open a new line of credit).

59. *Andrews*, 225 F.3d at 1065.

60. *See id.* (stating that the Imposter used her own information to apply for credit from Commercial Credit, except she used Andrews' social security number and misspelled Adelaide Andrews' first name as "Adeliade").

TRW furnished Andrews' credit reports to each creditor after the first initial, last name, and social security number on the credit applications matched the information contained in TRW's credit reports.<sup>61</sup> Of those applications, only the cable company accepted the Imposter's request for a line of credit.<sup>62</sup> Although the Imposter paid the cable company's minimum payment for a number of months, eventually she let the account become delinquent.<sup>63</sup> The cable account was sent to a collection agency, which pursued Andrews.<sup>64</sup>

Andrews became aware of the identity theft on May 31, 1995, when she inquired about refinancing the mortgage on her home.<sup>65</sup> The loan officer obtained a credit report that showed the fraudulent inquiries<sup>66</sup> made on Andrews' accounts at both TRW and Trans Union, including a notation that Andrews' had defaulted on her credit account with Dillard's department store.<sup>67</sup> As a result of the delinquent account listing on her credit report, Andrews was denied the loan refinancing terms that she desired.<sup>68</sup> Afterwards, Andrews experienced emotions common to identity theft victims: she was "shocked and humiliated by the allegation that she was neither creditworthy nor truthful about her financial dealings."<sup>69</sup>

---

61. See *TRW, Inc. v. Andrews*, 534 U.S. 19, 24 (2001) (explaining that when the TRW computers registered a match, Andrews' file was provided to the requester); see also *Andrews*, 225 F.3d at 1065 (declaring that TRW treated the Imposter's credit inquiries as if made by Adelaide Andrews).

62. *TRW*, 534 U.S. at 24.

63. Respondent's Brief at 5, *TRW* (No. 00-1045); see also Brief of Amici Curiae the Nat'l Assoc. of Consumer Advocates et al. at 9, *TRW* (No. 00-1045) (explaining that paying the minimum balance on fraudulent credit lines is one technique identity thieves use to avoid discovery).

64. *Andrews*, 225 F.3d at 1065.

65. See *Andrews v. Trans Union Corp.*, 7 F. Supp. 2d 1056, 1064 (C.D. Cal. 1998) (explaining that Andrews discovered the identity theft when she spoke to a loan officer at Home Savings of America).

66. See CALPIRG/PRIVACY RIGHTS CLEARINGHOUSE, NOWHERE TO TURN: VICTIMS SPEAK OUT ON IDENTITY THEFT 12 (May 2000) [hereinafter NOWHERE TO TURN] (explaining that credit bureaus record every inquiry into a consumer's account, even if the application for credit is ultimately denied), available at <http://www.privacyrights.org/ar/idtheft2000.htm> (last visited July 21, 2002). Therefore, the imposter's fraudulent applications for credit were listed on Andrews' credit report.

67. See *Andrews*, 7 F. Supp. 2d at 1064 (detailing the facts of Andrews' loan inquiry in which Home Savings of America obtained a credit report for Andrews that reflected the Imposter's activities).

68. See *id.* (explaining that Andrews abandoned the loan application she filed at Home Savings of America and obtained financing from Merrill Lynch at a higher interest rate); see also Respondent's Brief at 6, *TRW* (No. 00-1045) (discussing the fact that Home Savings of America denied Andrews' loan application because of recent negative credit history).

69. Respondent's Brief at 6, *TRW* (No. 00-1045).

Although TRW corrected her file,<sup>70</sup> the violation of privacy<sup>71</sup> still haunted Andrews for a year after it was discovered.<sup>72</sup> The collection agency continued to pursue her, and she was denied credit once again due to the misinformation contained in the TRW credit report.<sup>73</sup> Andrews also alleged that TRW's breach of privacy led to emotional distress and exacerbated a pre-existing chronic medical condition.<sup>74</sup>

*B. The Lower Courts' Analyses*

Andrews brought suit against TRW and Trans Union Corp. on October 21, 1996, alleging violations of the FCRA.<sup>75</sup> The FCRA was enacted to balance the competing interests of the credit reporting industry and consumers.<sup>76</sup> While providing credit is essential to the health of the economy, consumers are concerned with maintaining the accuracy and privacy of their credit histories.<sup>77</sup> The FCRA reconciles these goals by requiring credit reporting agencies to adopt and maintain reasonable procedures to ensure accuracy and privacy.<sup>78</sup>

---

70. *See id.* at 6-7 (implying that TRW's attempts to clear Andrews' credit file proved insufficient); *Andrews*, 7 F. Supp. 2d at 1064 (explaining that Trans Union's credit report continued to show the fraudulent Dillard's inquiry and stating that Andrews filed an inadequate reinvestigation claim only against Trans Union, and not against TRW).

71. One of the purposes of the FCRA is "to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality and a respect for consumer's right to privacy." 15 U.S.C. § 1681(a)(4). When a consumer reporting agency discloses a consumer's information in violation of a provision of the FCRA (i.e. disclosing information for an impermissible purpose), it is a violation of that consumer's privacy.

72. *See* Respondent's Brief at 7, *TRW* (No. 00-1045) (stating that Andrews was "vexed throughout the next year by resurgent problems springing from TRW's and Trans Union Corporation's lax consumer reporting procedures").

73. *See id.* (describing how TRW "purported[ly]" took procedures to correct her files, but insisting that a collection agency continually "hounded" her and that Andrews was "confronted with resurgent misinformation"). For example, the resurgent misinformation contained in Andrews' TRW credit report complicated her application for credit when she changed residences. *Id.*

74. *See id.* (explaining that Andrews experienced anger, frustration, worry, and mental anguish, such that her rheumatologist testified as to the exacerbation of Andrews' chronic pre-existing medical condition).

75. *Andrews*, 7 F. Supp. 2d at 1060-61. In her complaint, Andrews alleged improper disclosure under 15 U.S.C. §§ 1681b and 1681e(a), inadequate procedures to maintain accuracy under 15 U.S.C. § 1681e(b), improper reinvestigation by Trans Union in derogation of 15 U.S.C. § 1681i(a), and violation of California's Unfair Trade Practices Act. *Id.* *See generally* Fair Credit Reporting Act, 15 U.S.C. §§ 1601, 1681-1681u (2000) (outlining the obligations of credit reporting agencies).

76. *See* 15 U.S.C. § 1681(a)(1)-(4) (outlining congressional findings that although credit reporting agencies are important to maintaining public confidence in the banking system, they also must respect consumer privacy).

77. *See id.* (stating that inaccuracies would undermine public confidence in the banking system).

78. *See id.* § 1681(b) (requiring credit reporting agencies to establish "reasonable

Towards this end, the FCRA authorizes disclosure of consumer reports only for certain limited and permissible purposes,<sup>79</sup> requires parties to notify consumers if adverse action will be taken on the basis of their credit reports,<sup>80</sup> provides consumers with the right to access information,<sup>81</sup> and creates a procedure for disputing inaccuracies.<sup>82</sup> The FCRA also grants a private right of action to consumers but only for those seeking civil liability damages for willful, knowing, or negligent noncompliance with the FCRA's provisions.<sup>83</sup>

First, Andrews claimed that TRW and Trans Union violated § 1681e(a) of the FCRA,<sup>84</sup> which prohibits disclosure of consumer reports to third parties except for certain enumerated permissible purposes, such as credit transactions in which the consumer is involved.<sup>85</sup> Andrews alleged that the agencies did not supply credit reports for a permissible purpose because there was no reasonable belief that she was the consumer "involved" in the transactions.<sup>86</sup> Second, Andrews claimed that the agencies violated § 1681e(b) of the FCRA,<sup>87</sup> which requires credit reporting agencies to "follow

---

procedures" that promote and ensure accuracy, confidentiality, and proper utilization of the credit information received while at the same time remaining "fair and equitable" to the consumer); *see also* *July 12, 2000 Hearings, supra* note 20, at 73 (statement of Stuart Pratt, Vice President of Government Relations, Associated Credit Bureau) (providing an overview of the purposes and uses of the FCRA).

79. *See* 15 U.S.C. § 1681b (enumerating the permissible purposes for which a credit report can be disclosed, including credit transactions involving the consumer, employment purposes, and underwriting of insurance).

80. *See id.* § 1681m (attempting to safeguard consumers by imposing certain duties on persons who utilize information contained in credit reports).

81. *See id.* § 1681g(a)(1) (setting forth requirements that every consumer reporting agency shall "clearly and accurately disclose to the consumer . . . [a]ll information in the consumer's file at the time of the request").

82. *See id.* § 1681i (detailing procedures to be taken in the event of a "disputed accuracy").

83. *See id.* §§ 1681n-o (allowing a private right of action for noncompliance); *see also id.* § 1681h(e) (limiting liability of credit reporting agencies, among others, unless the allegation involves willful, knowing, or negligent noncompliance under 15 U.S.C. § 1681n-o).

84. *Andrews v. Trans Union Corp.*, 7 F. Supp. 2d 1056, 1061 (C.D. Cal. 1998).

85. *See* 15 U.S.C. § 1681e(a) (providing that "[n]o consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in section 1681b of this title."). Section 1681b authorizes certain limited conditions and circumstances under which a consumer's credit report may be produced to a third party, including the allowance that a credit reporting agency may furnish a consumer report "to a person which it has reason to believe . . . intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished . . ." *Id.* § 1681b(a)(3)(A).

86. *See Andrews*, 7 F. Supp. 2d at 1065 (alleging that Andrews' file was not furnished for a permissible purpose because its disclosure was based on a credit application by the Imposter).

87. *See id.* at 1071 (claiming injury under 15 U.S.C. § 1681e(b), which imposes a higher standard of accuracy on credit reporting agencies than is required by the

reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.”<sup>88</sup> Trans Union and TRW disclosed Andrews’ credit report to the five creditors when key identifiers, such as her first name, current address, and date of birth, did not match.<sup>89</sup> She alleged that these disclosures facilitated her identity theft, and she sought injunctive relief, punitive damages and compensation for the time, money, inconvenience, and emotional distress that TRW had allegedly caused.<sup>90</sup>

On the first claim of improper disclosures under § 1681e(a), the district court granted partial summary judgment for the credit reporting agencies, based on the statute of limitations.<sup>91</sup> Section 1681p of the FCRA allows an action against a credit reporting agency to be brought “within two years from the date on which the liability arises,” unless the defendant has made a material and willful misrepresentation of information.<sup>92</sup> In that event, the two-year statute of limitations begins when the plaintiff discovers the misrepresentation.<sup>93</sup>

TRW argued that because the first two disclosures to FCNB and Prime Cable were made more than two years before the suit was filed, those disclosures could not give rise to any liability.<sup>94</sup> Andrews argued that the discovery rule<sup>95</sup> should apply and that the statute of

---

improper disclosure rule under § 1681e(a)).

88. 15 U.S.C. § 1681e(b).

89. See *Andrews*, 7 F. Supp. 2d at 1063 (describing the Imposter’s various credit inquiries and highlighting the multiple occasions when the Imposter lacked, or failed to provide, accurate identifying information about the plaintiff, Adelaide Andrews).

90. See *TRW*, 534 U.S. at 25 (describing the injuries that Andrews alleged resulted from the law security at the credit reporting agencies).

91. See *Andrews*, 7 F. Supp. 2d at 1067 (holding that the claim was barred by § 1681p).

92. 15 U.S.C. § 1681p.

An action to enforce any liability created under this title may be brought in any appropriate United States district court without regard to the amount in controversy, or in any other court of competent jurisdiction, within two years from the date on which the liability arises, except that where a defendant has materially and willfully misrepresented any information required under this title to be disclosed to an individual and the information so misrepresented is material to the establishment of the defendant’s liability to that individual under this title, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

*Id.*

93. *Id.*

94. *Andrews*, 7 F. Supp. 2d at 1066.

95. See generally 51 AM. JUR. 2D *Limitation of Actions* § 179 (2000) (defining the discovery rule as an equitable principle in which a plaintiff’s claim will not accrue until he or she discovers or should have discovered that they had a cause of action or until the plaintiff discovered or should have discovered all the elements of the cause

limitations did not begin until she knew or should have known of the improper disclosures.<sup>96</sup> The district court stated that § 1681p clearly established a two-year statute of limitations,<sup>97</sup> but examined whether § 1681p could be read to include an implied discovery rule.<sup>98</sup>

The district court concluded that the plain language of the statute precluded the application of the discovery rule.<sup>99</sup> The court reasoned that the existence of the exception in § 1681p—applying the discovery rule when the defendant made a material and willful misrepresentation—implied that Congress did not intend for the discovery rule to apply to all FCRA cases.<sup>100</sup> It explained that holding otherwise would depart from decisions in other circuits that have refused to toll the statute of limitations in FCRA cases until the discovery of the injury.<sup>101</sup> Therefore, Andrews' claim of improper disclosure of her credit report to the first two creditors (FCNB and Prime Cable) was time barred.<sup>102</sup>

On appeal, the Ninth Circuit reversed the district court's decision that barred Andrews' claims.<sup>103</sup> The court recognized Ninth Circuit precedent that held that, as a general rule, "a federal statute of limitations begins to run when a party knows or has reason to know that she was injured."<sup>104</sup> Relying on Supreme Court precedent, the Ninth Circuit explained that "the equitable doctrine of discovery 'is read into every federal statute of limitations'" unless Congress has expressly legislated otherwise.<sup>105</sup> Finding no such expression from

---

of action).

96. *Andrews*, F. Supp. 2d at 1066.

97. *Id.*

98. *Id.*

99. *Id.*

100. *See id.* (relying on the premise that "[w]here 'Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent.'" (quoting *Andrus v. Glover Constr. Co.*, 446 U.S. 608, 616-17 (1980))).

101. *See id.* (stating that the Third, Seventh and Tenth Circuits all refused to apply a general discovery rule to § 1681p (citing *Clark v. State Farm Fire & Cas.*, 54 F.3d 669, 672-73 (10th Cir. 1995); *Rylewicz v. Beaton Servs., Ltd.*, 888 F.2d 1175, 1181 (7th Cir. 1989); *Houghton v. Ins. Crime Prevention Inst.*, 795 F.2d 322, 325 (3d Cir. 1986))).

102. *Id.* The district court held that, even though the reports were disclosed to the Imposter, the remaining disclosures were proper because they were made for permissible purposes under the FCRA and because TRW had procedures reasonably designed to prevent impermissible disclosures. *Id.* at 1068-69. Andrews' second claim of inaccuracy was tried by a jury who found for TRW. *TRW, Inc. v. Andrews*, 534 U.S. 19, 24 n.3 (2001). Adelaide Andrews settled her claims with Trans Union; therefore, they did not proceed.

103. *Andrews v. TRW, Inc.*, 225 F.3d 1063, 1067 (9th Cir. 2000), *rev'd*, 534 U.S. 19 (2001).

104. *Id.* at 1066 (quoting *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1266 (9th Cir. 1998)).

105. *See id.* at 1067 (quoting *Holmberg v. Armbrecht*, 327 U.S. 392, 397 (1946)), in

Congress, the Ninth Circuit applied a general discovery rule.<sup>106</sup> The court's decision was also an attempt to be consistent with an earlier decision in which the discovery rule was applied to actions under an analogous statute.<sup>107</sup> Thus, Andrews' claims against TRW for improper disclosure were reinstated.<sup>108</sup>

### C. *The Supreme Court Opinion*

The Supreme Court granted certiorari to resolve the issue of whether the statute of limitations in an action against a credit reporting agency under the FCRA begins when the plaintiff discovers the violation (the injury discovery rule) or when the violation initially occurs (violation occurrence rule).<sup>109</sup> Andrews certainly faced an uphill battle; at least three circuits had already held that a general discovery rule does not apply to toll the statute of limitations in the FCRA.<sup>110</sup> The Supreme Court rejected the Ninth Circuit's presumption that a discovery rule applies for all federal statute of limitations unless Congress expressly legislates otherwise.<sup>111</sup> The Court concluded that congressional intent to deny a general discovery rule does not need to be explicit, as the Ninth Circuit had held, but can be implied from the text and structure of the statute.<sup>112</sup>

---

which the discovery rule was applied to a cause of action for fraud, and stating that the language of the FCRA and decisions of other circuits should yield to this Supreme Court principle).

106. *See id.* (holding that Andrews' claims were not barred).

107. *See id.* (citing *Englerius v. Veterans Admin.*, 837 F.2d 895, 898 (9th Cir. 1988), which interpreted the Privacy Act to include a discovery rule).

108. *See id.* (finding that none of Andrews' claims were stale when she brought suit). The Ninth Circuit also reversed the district court holding that TRW's disclosures were permissible under the FCRA. *Id.* The Ninth Circuit, however, affirmed the district court on the accuracy claim, dismissing her accuracy claim under § 1681e(b), by finding that TRW had procedures reasonably designed to prevent impermissible disclosures. *Id.* at 1068.

109. *TRW, Inc. v. Andrews*, 532 U.S. 902 (2001); *see TRW* 534 U.S. 19, 26 (2001) (writing that the Court would look at the case to resolve a conflict between the Ninth Circuit and four other circuits: the Third, Seventh, Tenth, and Eleventh).

110. *See TRW*, 534 U.S. at 26 (citing *Clark v. State Farm Fire & Cas.*, 54 F.3d 669, 672-73 (10th Cir. 1995); *Rylewicz v. Beaton Servs., Ltd.*, 888 F.2d 1175, 1181 (7th Cir. 1989); *Houghton v. Ins. Crime Prevention Inst.*, 795 F.2d 322, 325 (3d Cir. 1986); *Clay v. Equifax*, 762 F.2d 952, 961 (11th Cir. 1985)).

111. *See id.* (stating that "beyond doubt, the Court has never endorsed the Ninth Circuit's view that Congress can convey its refusal to adopt a discovery rule only by explicit command . . .").

112. *See id.* (stating that the Ninth Circuit erred "in holding that a generally applied discovery rule control[led the] case").

The Court stated that it only recognized an injury discovery rule in certain circumstances.<sup>113</sup> First, the Court has recognized the discovery rule in cases of fraud or concealment.<sup>114</sup> In cases of fraud, the statute of limitations is tolled until discovery of the injury because the plaintiff is ignorant of it without any fault or lack of diligence on his part.<sup>115</sup> Second, the Court has applied the discovery rule “where the cry for [such a] rule is loudest.”<sup>116</sup> For example, in cases of latent disease or medical malpractice, the Court has implied a discovery rule, but only where a claim is brought under what it considers “humane” legislation.<sup>117</sup> While noting that lower federal courts have applied the discovery rule when a statute is silent on the issue,<sup>118</sup> the Supreme Court has refused to follow their lead.<sup>119</sup> The Court concluded that because the FCRA is not silent on the issue and “does not govern an area of the law that cries out” for its application, the discovery rule does not apply.<sup>120</sup>

The Supreme Court looked to statutory construction to show that § 1681p precluded the discovery rule<sup>121</sup> and relied on the principle of “*expressio unius est exclusio alterius*” to support its argument.<sup>122</sup> The Court accepted the petitioner’s and the district court’s argument that when a statute explicitly enumerates certain exceptions, additional exceptions are not to be implied.<sup>123</sup> The Court held that “Congress

---

113. *Id.*

114. *Id.* (citing *Holmberg v. Armbrrecht*, 327 U.S. 392, 397 (1946)).

115. *See id.* (explaining that although *Holmberg* held that equity tolls the statute of limitations in cases of fraud, it did not “establish a general presumption applicable across all contexts”).

116. *Id.* (alteration in original) (quoting *Rotella v. Wood*, 528 U.S. 549, 555 (2000)).

117. *See id.* at 37 (Scalia, J., concurring) (referring to cases of medical malpractice and latent disease in which the court has recognized the discovery rule because the “humane” legislation, under which plaintiffs’ claims were brought, could not have been interpreted as being so unfair to plaintiffs in those circumstances (citing *Urie v. Thompson*, 337 U.S. 163, 170 (1949))); *see, e.g.*, *Rotella v. Wood*, 528 U.S. 549 (2000) (recognizing the injury discovery rule in medical malpractice cases, but refusing to apply it in a RICO action); *United States v. Kubrick*, 444 U.S. 111, 122 (1979) (advocating an injury and causation discovery rule, under the Federal Torts Claims Act, in which the statute of limitations begins to run when a plaintiff knows he has been hurt and can identify the defendant).

118. *See TRW*, 534 U.S. at 27.

119. *See id.* (stating that “we have not adopted that position as our own.”).

120. *See id.* at 28 (suggesting that the FCRA is not silent because § 1681p addresses the statute of limitations issue, and that the FCRA is not considered humane legislation).

121. *Id.*

122. *Id.*; *see also* BLACK’S LAW DICTIONARY 602 (7th ed. 1999) (defining the Latin phrase as a “canon of construction holding that to express or include one thing implies the exclusion of the other, or of the alternative”).

123. *See TRW*, 534 U.S. at 28-29 (explaining that enumerating exceptions indicate congressional intent to preclude courts from including additional exceptions not listed); *see also* Petitioner’s Brief at 21, *TRW* (No. 00-1045) (advocating a traditional

implicitly excluded a general discovery rule by explicitly including a more limited one.”<sup>124</sup>

Relying on the text of FCRA § 1681p, the Court explained that applying a general discovery rule would render the misrepresentation exception “superfluous.”<sup>125</sup> As the Court explained, in an average case, the consumer will not discover an improper disclosure until she requests a credit report.<sup>126</sup> If the credit reporting agency conceals the information, then both the discovery rule and the misrepresentation exception would toll the statute of limitations.<sup>127</sup> When the concealed disclosure is discovered, the statute of limitations would begin to run under either rule.<sup>128</sup> According to a hallmark of statutory interpretation, no word in a statute shall be superfluous, unless it cannot be prevented.<sup>129</sup> Because the Court found that applying a general discovery rule would make the misrepresentation exception meaningless, it refused to extend the discovery rule beyond cases of misrepresentation or concealment.<sup>130</sup>

Finally, the Court examined the legislative history of the statute of limitations in the FCRA and reaffirmed its conclusion that Congress did not intend to apply a general discovery rule to the FCRA.<sup>131</sup> Andrews argued that initial drafts of the FCRA had expressly included language that tolled the statute of limitations until the “date of the occurrence of the violation.”<sup>132</sup> Because that language was replaced with the “liability arises” language, Andrews argued that Congress did not intend for the statute of limitations to begin when the violation occurred.<sup>133</sup> This argument did not persuade the Court because the legislative history also showed that lawmakers rejected testimony that encouraged them to begin the running of the statute of limitations when the violation was discovered.<sup>134</sup> In addition, the

---

commencement rule because the only exceptions Congress intended are expressly stated).

124. See *TRW*, 534 U.S. at 28 (stating that reading the exception into the rule would distort the statute’s text by turning the exception into the rule).

125. *Id.* at 29.

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.* at 31 (citing *Duncan v. Walker*, 533 U.S. 167, 174 (2001)).

130. *Id.*

131. *Id.* at 32-33.

132. *Id.* at 32; see also Respondent’s Brief at 26, *TRW* (No. 00-1045) (suggesting that initial drafts of the FCRA would have expressly applied a violation occurrence rule).

133. See Respondent’s Brief at 28, *TRW* (No. 00-1045) (arguing that the final version’s lack of violation occurrence language is evidence of the congressional intent “to choose a more accommodating type of statute of limitations”).

134. See *TRW*, 534 U.S. at 33 (explaining that the legislative history is not dispositive).

Court noted that the misrepresentation exception was adopted at the same time the “date of occurrence” language was deleted.<sup>135</sup> The Court explained that it was doubtful that Congress would create an exception and adopt a general discovery rule simultaneously.<sup>136</sup>

This Supreme Court decision is devastating for identity theft victims as well as consumer protection advocates.<sup>137</sup> The Court’s interpretation of the statutory language creates a significant burden on the victim of identity theft.<sup>138</sup> Running the statute of limitations from the time of the initial FCRA violation forces victims to bear significant losses.<sup>139</sup>

### III. THE LEGAL SYSTEM AND THE CREDIT INDUSTRY CREATE BURDENS ON IDENTITY THEFT VICTIMS

Despite the Supreme Court’s ruling, the prevalence of identity theft, the disastrous effects it has on victims and its connection to the credit reporting agencies, are evidence that the FCRA does cover an area of the law that “cries out” for application of the discovery rule.<sup>140</sup> In 1997, actual losses from identity theft to victims and financial institutions totaled \$745 million.<sup>141</sup> This figure, however, does not reflect the “human costs” suffered by the victims of identity theft, as cases like Adelaide Andrews’ reflect.<sup>142</sup> While a victim of consumer identity theft will not be held liable for the debts incurred by identity thieves,<sup>143</sup> they bear the burden of regaining their financial health and restoring their credit history.<sup>144</sup> A study of sixty-six identity theft

---

135. *Id.*

136. *Id.*

137. *See Borrowers Beware, supra* note 44, at 6 (objecting to Congress and the judiciary’s decision to limit the discovery rule to cases of misrepresentation).

138. *See id.* (explaining that victims could be barred from bringing an action to enforce the FCRA provisions if they do not review credit reports every two years).

139. *See id.* (arguing that the judiciary’s reliance on statutory construction is understandable but that Congress should reexamine its position because victims will lose their opportunity to recover damages for improper disclosures).

140. *See id.* (calling for Congress to consider the needs of victims of identity theft when applying a statute of limitations to the FCRA).

141. GAO REPORT, *supra* note 27, at 1.

142. *See id.* at 22 (explaining that emotional, financial, and opportunity costs can be substantial and that identity theft victims report feeling “violated”); *see also* NOWHERE TO TURN, *supra* note 67, at 4 (explaining that stress, emotional trauma, time lost, and damaged credit reputation, not the financial aspect of the fraud, were most difficult).

143. *See* 15 U.S.C. § 1643(a) (2000) (limiting liability of a cardholder for unauthorized credit card use to fifty dollars).

144. *See July 12, 2000 Hearings, supra* note 20, at 30 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (explaining that time and effort required to restore credit history can be frustrating); *see also* Margaret Mannix, *Getting Serious About Identity Theft*, U.S. NEWS & WORLD REPORT, Nov. 8, 1999, at 88 (explaining that despite the FTC clearinghouse, the burden of clearing credit history is still on the

cases reported that it took an average of 175 hours and \$808 in out-of-pocket expenses to remedy the effects of consumer identity theft.<sup>145</sup> Victims suffer from loss of time and money, as well as stress, anxiety, embarrassment, and frustration.<sup>146</sup> As Adelaide Andrews experienced, victims are continuously hounded by collection agencies and are refused credit because of the work of an imposter.<sup>147</sup> Besides the emotional trauma associated with a violation of privacy, victims face two primary burdens in their quest to rebuild their credit histories: the statute of limitations for actions against credit reporting agencies and the inefficient procedures of the credit industry.<sup>148</sup>

A. *Burdens Imposed Through the Legal System*

By ruling that the “text and structure” of the FCRA would not allow the courts to imply a discovery rule,<sup>149</sup> the Supreme Court disregarded the new reality of identity theft and the plight of the victim.<sup>150</sup> Considering the recent rise in identity theft, Congress should revisit the statute of limitations issue in the FCRA and make it better reflect the true reality victims face.<sup>151</sup> The arguments in favor of applying the violation occurrence rule to run the statute of limitations ignore the unique nature of identity theft,<sup>152</sup> where many identity theft victims

---

victim).

145. See NOWHERE TO TURN, *supra* note 67, at 1 (explaining the findings of a study, conducted by CALPIRG and Privacy Rights Clearinghouse, on the obstacles victims face when trying to resolve identity theft cases).

146. See *July 12, 2000 Hearings*, *supra* note 20, at 32 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (stating that victims suffer anxiety and frustration because it can take years to restore their good credit history).

147. See Martha Sabol, *The Identity Theft and Assumption Deterrence Act of 1998 Do Individual Victims Finally Get Their Day in Court?*, 11 LOY. CONSUMER L. REV. 165, 167-68 (1999) (describing the difficult and humiliating process of rectifying a credit history).

148. See Morphy, *supra* note 17 (explaining that the statute of limitations and the poor procedures designed by the credit industry make a victim’s recovery difficult); see also *Borrowers Beware*, *supra* note 44, at 6 (recognizing the additional burden the statute of limitations decision creates for an already difficult and lengthy process of rectifying an erroneously negative credit history).

149. See *TRW, Inc. v. Andrews*, 534 U.S. 19, 28 (2001) (concluding that the text and structure of § 1681p “evinces Congress’ intent to preclude judicial implication of a discovery rule”).

150. See Brief of Amici Curiae the Nat’l Assoc. of Consumer Advocates et al. at 10-11, *TRW* (No. 00-1045) (arguing that the credit reporting agencies have been ineffective in combating identity theft or assisting victims).

151. See *Borrowers Beware*, *supra* note 44, at 6 (advocating an amendment to the FCRA statute of limitations).

152. See Brief of Amici Curiae the Nat’l Assoc. of Consumer Advocates et al. at 12, *TRW* (No. 00-1045) (arguing that because identity theft victims do not learn of the crime for years, it would be unreasonable for the statute of limitations to begin running at the time of violation).

may not know the statute of limitations has started to run.<sup>153</sup> Although forty-five percent of victims discover the identity theft within a month, March 2001 data reported that twenty percent of victims do not realize their identities have been stolen until two years after it occurs.<sup>154</sup> On average, it takes 12.5 months from the time an identity is stolen for the victim to realize it.<sup>155</sup> Upon notification of identity theft, it then takes victims an average of two years to clear a credit history.<sup>156</sup> In response to this data, TRW argued that the “vast majority” of identity theft victims discover their injuries before the statute of limitations has run out.<sup>157</sup> However, the purpose of the FCRA as a consumer protection statute will be thwarted if *any* consumers lose their rights to hold a credit reporting agency liable for improper disclosures.<sup>158</sup>

Many victims will also lose their opportunity to recover damages from a credit reporting agency for improper disclosures because, even if they discover the violation within the two-year window, they will not be able to file a claim before the statute of limitations expires.<sup>159</sup> Andrews argued that because the FCRA is not a strict liability statute, it can take nearly two years to gather the information

---

153. *See id.* (explaining that it would be an injustice for the statute of limitations to run before victims realize their identities have been stolen).

154. *See* FTC, IDENTITY THEFT VICTIM COMPLAINT DATA: FIGURES AND TRENDS ON IDENTITY THEFT, NOVEMBER 1999 THROUGH JUNE 2001 4 (2001) [hereinafter JUNE 2001 DATA] (providing percentages of identity theft victims and the corresponding length of time it takes before the theft was discovered and stating that almost half of victims discover the injury within a month); MARCH 2001 DATA, *supra* note 32, at Figure 8 (showing that twenty percent of victims learn of the problem two years after it occurs, which is significant compared to the forty-five percent who discover their identity theft within a month); *see also* FCRA Statute of Limitations Begins to Run at *Time of Identity Theft*, 38 BANKR. CT. DECISIONS 16, Nov. 27, 2001, at 5 (reviewing the oral arguments at the Supreme Court in which Andrews’ attorney stated that twenty percent of victims do not find out about the theft within two years).

155. JUNE 2001 DATA, *supra* note 154, at Figure 8; *see* MARCH 2001 DATA, *supra* note 32, at Figure 8 (stating that the average number of months between occurrence and discovery is fifteen months); *see also* Beth Givens, Director, Privacy Rights Clearinghouse, Identity Theft: The Growing Problem of Wrongful Criminal Records, Presentation at the SEARCH National Conference on Privacy, Technology and Criminal Justice Information (June 1, 2000) [hereinafter SEARCH Presentation] (explaining that it takes an average of fourteen months to detect an identity theft), available at <http://www.privacyrights.org/ar/wcr.htm> (last visited Aug. 3, 2002).

156. SEARCH Presentation, *supra* note 155.

157. *See* Petitioner’s Reply Brief at 14-15, TRW (No. 00-1045) (arguing that the traditional statute of limitations is adequate because most victims discover the injury within two years).

158. *See Borrowers Beware*, *supra* note 44, at 6 (arguing that the statute of limitations on the FCRA should reflect the overall purpose of the statute, which is to advance efficiency in the banking and financial system and protect consumer privacy).

159. *See* Brief of Amici Curiae the Nat’l Assoc. of Consumer Advocates et al. at 10, TRW (No. 00-1045) (explaining that a victim has to “determine what transpired” and wait months to receive records from creditors concerning the fraudulent accounts).

necessary to bring a suit.<sup>160</sup> Since the FCRA requires a showing of negligence, the discovery of an inaccuracy alone is not sufficient to bring a suit against a credit reporting agency.<sup>161</sup> As Andrews argued, filing a claim also requires an examination into the legal standard of care to determine whether the defendant was negligent.<sup>162</sup> Therefore, a claim can take a substantial amount of time to prepare in order to avoid Rule 11 sanctions.<sup>163</sup> The initial purpose of the FCRA was to protect consumers by requiring procedures to maintain accuracy of credit reports.<sup>164</sup> Applying the violation occurrence rule contradicts this consumer protection purpose because in many cases it can take the full two years to discover an identity theft or to file a claim.<sup>165</sup>

The Court's statutory construction analysis could also be challenged in light of the new crisis of identity theft.<sup>166</sup> As Andrews argued, § 1681p could be read to incorporate the discovery rule.<sup>167</sup> Section 1681p begins running the statute of limitations when "liability arises."<sup>168</sup> Relying on the common definition of "arise," Andrews argued that liability did not manifest itself until the victim became aware of the theft.<sup>169</sup> TRW, on the other hand, argued that

---

160. See Respondent's Brief at 42-43, *TRW* (No. 00-1045) (explaining it can take two years from the time a victim discovers the identity theft for a victim to be sufficiently informed to bring a valid claim).

161. See *id.* at 43 (explaining that an examination into negligence standards, once the theft has been discovered, is necessary to avoid a frivolous lawsuit).

162. See *id.* at 43 n.30 (explaining that obtaining information on the standard of care is difficult because the credit industry is large and information is difficult to obtain).

163. See *id.* (arguing that the plaintiff would need two years to gather information and construct a well-informed lawsuit); Fed. R. Civ. P. 11 (requiring sanctions for frivolous lawsuits that are not well grounded in fact or law). *But see* Petitioner's Reply Brief at 15, *TRW* (No. 00-1045) (arguing that respondent failed to explain why it would take so long to file suit).

164. See Respondent's Brief at 13, *TRW* (No. 00-1045) (quoting *Burnett v. New York Cent. R.R.*, 380 U.S. 424, 427 (1965) in which the Court emphasized the importance of considering the underlying purpose of a statute when interpreting a statute of limitations).

165. See Brief of Amici Curiae the Nat'l Assoc. of Consumer Advocates et al. at 13, *TRW* (No. 00-1045) (explaining that the violation occurrence rule would immunize credit reporting agencies from liability); see also *Borrowers Beware*, *supra* note 44, at 6 (explaining that the goal of protecting consumers would be better served by beginning the statute of limitations at the time of discovery).

166. See Respondent's Brief at 13, *TRW* (No. 00-1045) (arguing that the language of § 1681p could be read to apply the discovery rule).

167. See *id.* (proposing that if the common meaning of the word "arises" is applied to § 1681p, the statute expressly provides for the discovery accrual rule).

168. 15 U.S.C. § 1681p (2000).

169. See Respondent's Brief at 13, *TRW* (No. 00-1045) (applying the common definition of "arise" to the language of § 1681p and arguing that not a single element of TRW's liability "sprang up, came into notice, came up, or presented itself before May 31, 1995, when she first discovered any credit problem"). *But see* Petitioner's Brief at 15-16, *TRW* (No. 00-1045) (arguing that the liability arises at the time of the

traditionally a statute of limitations would begin when the plaintiff has a complete cause of action.<sup>170</sup> Since the cause of action is complete and the credit reporting agency becomes liable at the moment it makes an improper disclosure, the liability “arises” at that point.<sup>171</sup> To a victim of identity theft, however, the cause of action is not complete until the victim realizes a violation has occurred, which will be longer than two years in many cases.<sup>172</sup>

The credit reporting agencies claim that the language of other FCRA statutory provisions, namely the “notice” and “access” provisions, are consistent with and support the application of a violation occurrence rule.<sup>173</sup> The “notice” provision of the FCRA requires a creditor to inform the consumer promptly when any adverse action is taken and also identify the reporting agency that took such an action.<sup>174</sup> The “access” provision requires a credit reporting agency to provide any information needed by the consumer to correct the improper disclosure.<sup>175</sup> Therefore, the agencies argued, a plaintiff is well aware of the time the statute of limitations begins to run against a credit reporting agency, which makes a discovery rule unnecessary.<sup>176</sup>

---

initial improper disclosure because the FCRA provisions are violated at that time).

170. See Petitioner’s Brief at 14, *TRW* (No. 00-1045) (defining the traditional commencement rule, which begins the tolling of the statute of limitations once a person has been injured, regardless of whether the injury has been discovered).

171. See *id.* at 16 (explaining that at the time of the initial improper disclosure, the consumer’s privacy is invaded, the cause of action is complete, and the credit reporting agency becomes liable).

172. See Respondent’s Brief at 14, *TRW* (No. 00-1045) (illustrating how allowing the statute of limitations to run before the victim is aware of the identity theft and, thus, unable to bring an action is harsh and unreasonable).

173. See Petitioner’s Brief at 26, *TRW* (No. 00-1045) (arguing on behalf of credit reporting agencies that a discovery rule would conflict with other provisions of the FCRA and the overall statutory scheme). *But see* Respondent’s Brief at 40, *TRW* (No. 00-1045) (arguing that the notice and access provisions are ineffective).

174. See 15 U.S.C. § 1681m(a) (2000) (providing that “if any person takes any adverse action with respect to any consumer that is based in whole or in part on any information contained in a consumer report, the person shall—(1) provide . . . notice of the adverse action to the consumer” and (2) provide the name of the consumer reporting agency that furnished the report).

175. See *id.* § 1681g(a)(1) (stating that “[e]very consumer reporting agency shall, upon request . . . clearly and accurately disclose to the consumer: (1) all information in the consumer’s file at the time of the request . . . .”); see also Petitioner’s Brief at 27, *TRW* (No. 00-1045) (arguing that the access provision gives consumers the means to identify improper disclosures).

176. See Petitioner’s Brief at 27-28, *TRW* (No. 00-1045) (asserting that the provisions make the discovery rule inapplicable because they allow victims to discover inaccuracies in a timely fashion but also admitting that because the Act does not require notification for a request for an ordinary credit report, the Act does not automatically notify the consumer of every potential disclosure).

This argument, however, fails to take into account the techniques identity thieves use.<sup>177</sup> The notice provision does not adequately protect an identity theft victim because imposters usually submit a change of address immediately after applying for credit.<sup>178</sup> Therefore, notice of adverse action will be sent to the imposter's address or some other fraudulent address.<sup>179</sup> Because a credit reporting agency will usually accept a change of address without question, the victim will not receive notice of any adverse action.<sup>180</sup> For example, TRW committed four privacy violations before Andrews became aware of them.<sup>181</sup> Andrews realized the violations only when she tried to refinance her home, not through any notification from TRW.<sup>182</sup>

The access provision also fails to sufficiently protect a possible victim.<sup>183</sup> This provision only requires a credit reporting agency to disclose information when there is reason to suspect an improper disclosure.<sup>184</sup> With identity theft, however, the victim has no reason to suspect an improper disclosure until after much time has elapsed and when the statute of limitations may have run.<sup>185</sup>

The application of the violation occurrence rule in identity theft cases under the FCRA is further inappropriate because the potential plaintiffs have become victims through no fault of their own.<sup>186</sup> In other cases, the Supreme Court applied the injury discovery rule when the plaintiff was unaware of the injury for some time.<sup>187</sup> In

---

177. See Brief of Amici Curiae Nat'l Assoc. of Consumer Advocates et al. at 15, *TRW* (No. 00-1045) (arguing that an imposter often changes the address on accounts, preventing the victim from receiving notice).

178. *Id.*

179. *Id.*

180. *Id.*; see also Eric Rich, *Fraud Made Easy: The Credit Industry Does Little to Protect Consumers From Identity Theft*, HARTFORD COURANT, Mar. 18, 2001, at A8 (reporting that credit bureaus are not required to verify a change of address). If credit bureaus sent a confirmation of change of address, fraud could be prevented. *Id.*

181. See Respondent's Brief at 41, *TRW* (No. 00-1045) (noting that Andrews received no notice and was only made aware of the privacy violations ten months after the first violation).

182. See *id.* (explaining that only the Imposter received the notifications from the reporting agency because the Imposter had changed the address when opening the fraudulent accounts).

183. *Id.*

184. See *id.* (explaining that a consumer will request information and their credit file once there is reason to believe there has been an improper disclosure).

185. See *id.* at 42 (explaining that although identity theft victims are vigilant about obtaining records when they know their identities have been stolen, most will not have the knowledge that they should be suspicious until well after the violation occurred).

186. See *March 7, 2000 Hearings, supra* note 24, at 12 (statement of Maureen Mitchell, victim) (explaining that "[w]e were thrown into a financial quagmire through no carelessness on our part.>").

187. See, e.g., *Urie v. Thompson*, 337 U.S. 163, 167 (1949) (applying the injury discovery rule in a workers compensation case because the plaintiff could not have

*Holmberg v. Armbrrecht*,<sup>188</sup> the Court applied the discovery rule to a case of fraud.<sup>189</sup> The Court specifically stated “that where a plaintiff has been injured by fraud and ‘remains in ignorance of it without any fault or want of diligence or care on his part, the bar of the statute does not begin to run until the fraud is discovered.’”<sup>190</sup>

In *Urie v. Thompson*,<sup>191</sup> the Court examined whether the three-year statute of limitations in the Federal Employer’s Liability Act barred Urie’s claim for compensation for work-related silicosis, a pulmonary disease.<sup>192</sup> The Court stated that it was unlikely that “the humane legislative plan intended such consequences to attach to blameless ignorance.”<sup>193</sup> Similarly, in cases of medical malpractice, the Court has endorsed the injury discovery rule because a plaintiff often will not learn of the injury until some time after it occurs, despite any diligence the plaintiff used.<sup>194</sup>

In *United States v. Kubrick*,<sup>195</sup> a veteran brought a medical malpractice claim against a Veteran’s Administration hospital under the Federal Tort Claims Act.<sup>196</sup> The Court held that the two-year statute of limitations begins when the plaintiff knows of the existence and cause of his injury.<sup>197</sup> The statute of limitations is tolled until the plaintiff discovers that he may have a legal claim.<sup>198</sup> The Court distinguished between instances where a plaintiff’s injury is unknowable and the facts pertaining to causation are under the

---

known about his injury).

188. 327 U.S. 392 (1946).

189. *See id.* at 397 (applying the discovery rule in a case in which the plaintiff sued shareholders and later discovered that one shareholder had concealed his ownership interests). The Court applied the discovery rule to toll the statute of limitations for an action against the fraudulent shareholder based on equity principles. *Id.*

190. *Id.* (quoting *Bailey v. Glover*, 88 U.S. (21 Wall.) 342, 348 (1874)).

191. 337 U.S. 163 (1949).

192. *See id.* at 169 (rejecting defendant’s claim that Urie’s case should be barred by the statute of limitations because Urie could have contracted the disease as early as 1910).

193. *Id.* at 170.

194. *See United States v. Kubrick*, 444 U.S. 111, 122-24 (1979) (applying discovery rule in a case of medical malpractice); *see also* Brief of Amicus Curiae the FTC at 25, TRW (No. 00-1045) (explaining that in some cases the plaintiff will not learn of an injury until well after it is inflicted and sometimes diligence may be fruitless).

195. 444 U.S. at 111.

196. *See id.* at 113 (explaining that Kubrick sued under the Federal Torts Claim Act for loss of hearing he experienced after surgery at a Veteran’s Administration hospital); *see also* 28 U.S.C. § 2401(b) (2000) (barring any claim against the U.S. unless it is presented within “two years after such claim accrues” to the appropriate federal agency).

197. *See Kubrick*, 444 U.S. at 122 (holding that a plaintiff who knows of the facts and is aware of his injury will not benefit from a longer statute of limitations because it is his responsibility to inquire whether the facts establish a legal claim).

198. *See id.* (explaining that the plaintiff who knows he has been injured is no longer at the mercy of the defendants).

control of the defendant, and instances in which a plaintiff knows of his injury but not his legal rights.<sup>199</sup> In the latter, all the plaintiff must do is inquire as to whether he has a cause of action.<sup>200</sup> In *Kubrick*, the plaintiff knew of his injury, but did not know that he could have made a legal claim for medical malpractice.<sup>201</sup> Because he only needed to inquire about his legal rights, the court would not allow *Kubrick* to benefit from a longer statute of limitations.<sup>202</sup> The plaintiff's discovery of the facts of his injury began the running of the statute of limitations.<sup>203</sup> Although *Kubrick* was not allowed to benefit from a longer statute of limitations, the court did not rule out the possibility that the discovery rule could be applied in other cases brought under the Federal Tort Claims Act where the claimant did not possess the relevant facts about the injury.<sup>204</sup>

In these cases, the Acts under which the plaintiffs brought their claims were considered "humane" legislation for which it would be inequitable to run the limitations period from the time the violation of the Act occurred.<sup>205</sup> The Court in *TRW* refused to analogize Andrews' identity theft to these medical malpractice, disease and fraud suits, claiming that the FCRA does not cover an area of the law that "cries out" for the discovery rule in the same way.<sup>206</sup>

The new phenomenon of identity theft and the burdens innocent victims face demonstrate the need to regard the FCRA as "humane" legislation.<sup>207</sup> The plight of an identity theft victim is similar to that of the plaintiffs in cases of fraud or latent disease because identity theft

---

199. *See id.* (stating that "[w]e are unconvinced that for statute of limitations purposes a plaintiff's ignorance of his legal rights and his ignorance of the fact of his injury or its cause should receive identical treatment.").

200. *Id.*

201. *See id.* at 123 (explaining that *Kubrick* only needed to ask doctors whether his hearing loss was due to the treatment he received for surgery).

202. *See id.* (describing that the statute of limitations will not wait to run until plaintiff is aware that the injury was negligently inflicted).

203. *See id.* (explaining that to excuse the plaintiff from inquiring as to his cause of action would undermine the purpose of the statute of limitations).

204. *Id.* at 124.

205. *See TRW, Inc. v. Andrews*, 534 U.S. 19, 37 (2001) (Scalia, J., concurring) (explaining that the Court "could not imagine that legislation as 'humane' as the Federal Employers' Liability Act would bar recovery for latent medical injuries").

206. *See id.* (noting that cases where the statute of limitations should be suspended are limited in character and should be admitted with great caution); *see also Rotella v. Wood*, 528 U.S. 549, 555 (2000) (describing that the "cry for the rule is loudest" in medical malpractice claims).

207. *See March 7, 2000 Hearings, supra* note 24, at 12 (statement of Maureen Mitchell, victim) (describing that victims suffer financial and emotional trauma through no fault of their own, and stating that victims need to repeatedly fill out forms and affidavits that are required by individual merchants in order to prove their innocence).

victims are also “blamelessly ignorant” of the injury.<sup>208</sup> As cases like *Andrews* show, identity theft plagues consumers who have been vigilant in keeping their financial situations in good order.<sup>209</sup> Applying the principle set out in *Kubrick*, *Andrews* was aware of neither her injury nor her legal rights.<sup>210</sup> The defendants and the Imposter were the only parties that knew of the improper disclosures until *Adelaide Andrews* applied for a mortgage.<sup>211</sup> Therefore, according to the *Kubrick* rationale, the statute of limitations should not run until *Andrews* discovered the theft.<sup>212</sup>

In her brief, *Andrews* emphasized that the discovery rule also has been applied in cases where plaintiffs seek damages for both physical and economic harms.<sup>213</sup> In an identity theft case, the plaintiff suffers both economic and physical damages.<sup>214</sup> Because the injury discovery rule is not limited to a specific type of injury or plaintiff, equity commands application of the rule in identity theft cases as well.<sup>215</sup>

The Supreme Court found that the legislative history of the FCRA fails to show that the discovery rule could be implied in § 1681p.<sup>216</sup> Both *TRW* and *Andrews* found language in the legislative history of the FCRA that supported their differing views.<sup>217</sup> Any arguments

---

208. *See id.* (stating that the victim did nothing wrong but still incurred a negative credit history).

209. *See July 12, 2000 Hearings, supra* note 20, at 25 (statement of Michelle Brown, victim) (“It is astounding that my life long discipline to be a law abiding citizen and to have the diligence to establish perfect credit was reversed so easily, so quickly, simply because I represent the perfect victim in another’s eyes.”); *May 20, 1998 Hearings, supra* note 8, at 19 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC) (explaining that identity thieves usually seek to victimize people with good credit history so the scam works).

210. *Andrews v. Trans Union Corp.*, 7 F. Supp. 2d 1056, 1064 (C.D. Cal. 1998); *see United States v. Kubrick*, 444 U.S. 111, 122 (1979) (distinguishing plaintiffs who know they have been injured and those that are unaware of the injury).

211. *See Andrews*, 7 F. Supp. 2d at 1064 (describing how *Andrews* discovered that her identity had been stolen when she attempted to refinance the mortgage on her home).

212. *See Kubrick*, 444 U.S. at 122 (explaining that where facts are unavailable to plaintiff, the statute of limitations should be applied differently than where a plaintiff knows he is injured).

213. *See* Respondent’s Brief at 19, *TRW* (No. 00-1045) (arguing that *Zenith Radio Corp. v. Hazeltine Research, Inc.*, 401 U.S. 321, 339 (1971), stands for the proposition that a cause of action under the Clayton Act does not accrue until the plaintiff suffers and feels the effect of an injury).

214. *See id.* at 7 (describing the economic and physical stress *Andrews* experienced, such as the exacerbation of *Andrews*’ pre-existing rheumatoid arthritis).

215. *See id.* at 21 (arguing that the discovery rule has been applied irrespective of type of plaintiff or injury).

216. *TRW, Inc. v. Andrews*, 534 U.S. 19, 33 (2001).

217. *See* Respondent’s Brief at 27, *TRW* (No. 00-1045) (arguing that congressional intent to apply the discovery rule can be found because language that applied a violation occurrence rule was specifically deleted in the final version of the FCRA). *But see* Petitioner’s Brief at 36, *TRW* (No. 00-1045) (explaining that Congress was

based on the legislative history of the FCRA, however, would not be instructive because identity theft was not a “national crisis” in 1970 when the FCRA was enacted.<sup>218</sup> Considering the relatively new emergence of identity theft and the attention it has recently received from Congress, it is evident that reliance on legislative history would be misplaced.<sup>219</sup>

*B. Inefficient Procedures in the Credit Reporting Industry Impose Additional Burdens*

The statute of limitations is not the only burden victims of identity theft face.<sup>220</sup> The overall effect of any proposal to assist a victim in the remediation process will be limited because the credit industry’s procedures designed to help victims are inefficient.<sup>221</sup> The credit reporting agencies claim that the solution to identity theft is the more aggressive prosecution of identity thieves.<sup>222</sup> These agencies, however, play an integral role in preventing identity theft and in establishing better procedures to help victims clear their credit history.<sup>223</sup> Just as Andrews claimed, these entities “have both helped perpetuate identity theft and have made it difficult for victims to resolve their cases expeditiously.”<sup>224</sup> The procedures a victim must

---

aware of the problems of discovering injuries from credit reports and still rejected a proposal to apply a discovery rule).

218. See Hoar, *supra* note 9, at \*1 (claiming that identity theft is the “crime of the new millennium”).

219. See Petitioner’s Reply Brief at 13-14, *TRW* (No. 00-1045) (arguing that Congress was not concerned with identity theft in 1970).

220. See Morphy, *supra* note 17 (explaining that the statute of limitations and the credit industry’s procedures create obstacles for a victim of identity theft); see generally *IDENTITY THEFT WORKSHOP*, *supra* note 36 (recounting countless stories of victims who have been further victimized by the credit industry).

221. See *NOWHERE TO TURN*, *supra* note 67, at 1 (explaining that data shows a failure of law enforcement, government, and the credit industry to address the problem); see also Brief of Amici Curiae the Nat’l Assoc. of Consumer Advocates et al. at 13, *TRW* (00-1045) (stating that the consumers experience victimization after the initial fraud by creditors and credit reporting agencies).

222. See Rich, *supra* note 180, at A8 (explaining that the credit industry opposes reform); see also Press Release, Associated Credit Bureaus, Credit Reporting Industry Announces Identity Theft Initiatives (Mar. 14, 2000) (reporting that although the credit industry will implement voluntary initiatives, the problem will not be solved unless law enforcement aggressively prosecutes criminals), available at <http://www.cdiaonline.org/mediaroomdocs/IdentityTheftInitiatives.pdf> (last visited Aug. 3, 2002).

223. See *March 7, 2000 Hearings*, *supra* note 24, at 13 (statement of Maureen Mitchell, victim) (stating that credit reporting agencies and merchants have the “onus of responsibility”); see also *July 12, 2000 Hearings*, *supra* note 20, at 31 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (arguing that the credit industry must improve their victim assistance programs).

224. *NOWHERE TO TURN*, *supra* note 67, at 1-2; see *Privacy Rights Clearinghouse, Identity Theft Victim Stories: The Credit Grantor’s Facilitated the Identity Theft Crime* (stating that creditors “facilitate identity theft through their policies and practices”), available

follow to rectify the mess created by an identity thief can be confusing and time consuming.<sup>225</sup>

When a consumer becomes aware they are a victim of identity theft, he or she is told to notify, by phone and mail, each of the three credit reporting agencies and all creditors.<sup>226</sup> Thus, victims must prove their innocence to each company independently.<sup>227</sup> Many victims report that this process is particularly aggravating because "the victim of identity theft is assumed guilty until proven innocent."<sup>228</sup>

Victims of identity theft also have pointed to a series of inefficiencies and inconsistencies in reporting fraud to the credit reporting agencies.<sup>229</sup> First, each credit reporting agency has different procedures, requiring different information and documentation from victims.<sup>230</sup> Second, the credit reporting agencies do not communicate effectively, and a fraud alert or suspicious activity on one agency's report will likely be left out of another.<sup>231</sup> Third, despite the credit reporting agencies' obligation to remove inaccurate data,<sup>232</sup> fraudulent accounts often will reappear in a later

---

at <http://www.privacyrights.org/victim18.htm> (last visited Aug. 3, 2002).

225. See NOWHERE TO TURN, *supra* note 67, at 5 (reporting that seventy-eight percent of respondents indicated loss of time as their main concern stemming from identity theft).

226. See *July 12, 2000 Hearings*, *supra* note 20, at 9-10 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (describing the process of remedying the effects of identity theft).

227. See *March 7, 2000 Hearings*, *supra* note 24, at 11 (statement of Maureen Mitchell, victim) (explaining that she sent dozens of affidavits, letters, forms, and handwriting samples to credit reporting agencies, and needed to prove her innocence thirty different times to thirty different merchants).

228. *Id.*; see IDENTITY THEFT WORKSHOP, *supra* note 36, at 34 (remarks of Deborah North, victim) ("[T]hat was the beginning of a long process, a lot of work, and time, to prove your innocence . . . . You know, normally you're innocent until proven guilty, but in this case, it's the opposite.").

229. See generally *July 12, 2000 Hearings*, *supra* note 20, at 34 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (reviewing the most common complaint of victims of identity theft); IDENTITY THEFT WORKSHOP, *supra* note 36, at 34-55 (discussing how the procedures used by credit reporting agencies make recovery difficult).

230. See IDENTITY THEFT WORKSHOP, *supra* note 36, at 95 (remarks of Maxine Sweed, Experian Information Systems, Inc.) (noting all three agencies have different processes for handling consumer complaints of fraud); see also *Ways and Means Hearings*, *supra* note 2, at 14 (statement of Emeka Moneme, victim) (describing one of her frustrations as the lack of uniformity across the three credit bureaus).

231. See IDENTITY THEFT WORKSHOP, *supra* note 36, at 149 (remarks of Bhavna Bhagwakar, Volkswagen Financing Co.) (acknowledging that the lack of consistency between credit reporting agencies' fraud alerts can lead to mistake in the approval process).

232. See 15 U.S.C. §§ 1681i(a)(5)(A)-(C) (2000) (explaining that credit reporting agencies shall promptly delete inaccurate data and shall maintain procedures to prevent reappearance).

credit report, leading to continuous denials of credit for the victim.<sup>233</sup> Fourth, the credit bureaus do not monitor the number of inquiries made to an account<sup>234</sup> and often cannot readily give the victim the name and address of every company that made such an inquiry.<sup>235</sup>

Creditors' lack of security at the point of transaction creates an equally significant burden on the victim of identity theft.<sup>236</sup> Identity thieves can easily use pre-approved credit cards sent through the mail by banks and creditors.<sup>237</sup> Moreover, as Adelaide Andrews' case proves, many creditors approve transactions despite obvious mistakes made by the imposter.<sup>238</sup> Fraud alerts also are often ineffective because they are not prominently displayed.<sup>239</sup> Because the alert can appear on the last page of a report, creditors do not see it and continue to issue credit to the identity thief.<sup>240</sup> Currently, creditors

---

233. See *Ways and Means Hearings*, *supra* note 2, at 14 (statement of Emeka Moneme, victim) (recounting that she had to overcome the additional problem of reappearing deleted accounts); *NOWHERE TO TURN*, *supra* note 67, at 7 (explaining that one roadblock victims complained of was reappearance of fraudulent accounts); see also *IDENTITY THEFT WORKSHOP*, *supra* note 36, at 117 (remarks of Edmund Mierzwinski, U.S. Public Interest Research Group) (stating that reappearance should not happen because the 1996 amendments to FCRA created an individual's private right of action to sue credit bureaus if they failed to comply with reinvestigation procedures).

234. See Rich, *supra* note 180, at A8-A9 (explaining that credit bureaus do not monitor consumer profiles for obvious signs of identity theft); see also *March 7, 2000 Hearings*, *supra* note 24, at 17 (statement of Maureen Mitchell, victim) (stating that her credit report, reflecting twenty-five inquiries in sixty days, did not send a "red flag" to the credit reporting agency).

235. See *IDENTITY THEFT WORKSHOP*, *supra* note 36, at 36 (remarks of Nicole Robinson, victim) (recalling that only one credit reporting agency was able to immediately give the victim a list of recent inquiries).

236. See *NOWHERE TO TURN*, *supra* note 67, at 7 (noting that many victims claim that creditor negligence caused the problem and that "the credit industry had perpetuated, rather than prevented, the problem").

237. See Rich, *supra* note 180, at A8 (explaining that identity thieves steal pre-approved credit cards, change the address, and obtain more pre-approved cards at the new address, which leads to further damage).

238. See *Andrews v. TRW, Inc.*, 225 F.3d 1063, 1065 (9th Cir. 2000) (describing that the commercial credit agency approved credit based on obvious mistakes submitted by the Imposter, such as misspelling Andrews' first name); see also *Ways and Means Hearings*, *supra* note 2, at 10 (statement of Nicole Robinson, victim) (describing the various fraudulent names, addresses, and social security numbers that her imposter used); *March 7, 2000 Hearings*, *supra* note 24, at 19 (statement of Maureen Mitchell, victim) (explaining that some fraudulent applications contained blatant errors that should have alerted merchants).

239. *NOWHERE TO TURN*, *supra* note 67, at 14; see *Ways and Means Hearings*, *supra* note 2, at 10 (statement of Nicole Robinson, victim) (stating that some credit was extended even after fraud alerts were placed on credit reports); *March 7, 2000 Hearings*, *supra* note 24, at 15 (statement of Maureen Mitchell, victim) (recommending that fraud alerts appear on front page of a credit report).

240. See *IDENTITY THEFT WORKSHOP*, *supra* note 36, at 58 (remarks of Nicole Robinson, victim) (claiming that fraud alerts were put on her credit report in April, but the identity thief had opened new accounts in May and June); see also *July 12, 2000 Hearings*, *supra* note 20, at 30 (statement of Michelle Brown, victim) (stating

are not liable for disregarding a fraud alert, and the victim must wait to dispute the unauthorized charges.<sup>241</sup> Because the loss from identity theft is insignificant to creditors, they lack any incentive to pursue identity theft cases.<sup>242</sup>

Finally, a lack of communication with creditors places one of the most significant burdens on victims.<sup>243</sup> Obtaining the fraudulent billing statement and credit applications as evidence of the fraud is difficult.<sup>244</sup> While creditors are required to send the victim a fraud affidavit to verify the fraudulent accounts, this does not always occur.<sup>245</sup> Not only is it difficult to request and receive a fraud affidavit,<sup>246</sup> but victims must also complete a separate affidavit for each creditor, each of which requires similar information.<sup>247</sup> It is apparent from victim complaints that even if victims like Adelaide Andrews had filed their claims within the statute of limitations, they would be further victimized by the credit industry's lax security procedures.<sup>248</sup> One can only speculate as to how the needless trauma that Adelaide Andrews and many other victims suffered, could have been prevented had the credit industry's procedures and policies been more secure, effective, and consumer-friendly.

---

that fraud alerts should be clearly posted and fines should be imposed on creditors that disregard the fraud alert).

241. See Rich, *supra* note 180, at A8 (reporting there is no penalty for ignoring a fraud alert); see also 15 U.S.C. § 1681I (2000) (explaining procedures for disputing information on a consumer report).

242. See Katherine Millett, *Self Preservation to Restore Her Good Name, Elizabeth Knowles Was Up Against Both an Identity Thief and Official Indifference*, CHI. TRIB., Aug. 19, 2001, (Magazine), at 12 (stating that according to a Ford Motor Credit spokesman, "[f]or the company to expend its resources on an identity theft case, . . . the case must involve a big loss, diligent police investigators, a committed prosecutor and a victim who is willing to devote the time needed to be an effective witness.").

243. See *March 7, 2000 Hearings*, *supra* note 24, at 11 (statement of Maureen Mitchell, victim) (explaining that she encountered "answering machine hell" when contacting creditors).

244. See IDENTITY THEFT WORKSHOP, *supra* note 36, at 49 (remarks of Nicole Robinson, victim) (describing the difficulties in obtaining fraudulent bills and affidavits from the creditors); see also *Ways and Means Hearings*, *supra* note 2, at 14 (statement of Emeke Moneme, victim) (stating that none of the thirteen letters she has written to creditors have been answered and the fraudulent information remains on her report).

245. See IDENTITY THEFT WORKSHOP, *supra* note 36, at 50 (remarks of Joe Genera, victim) (reporting that many creditors have failed to send an affidavit, even though they are required to do so).

246. See *id.* (claiming that only five out of fourteen creditors sent him an affidavit).

247. See *March 7, 2000 Hearings*, *supra* note 24, at 47 (question of Sen. Dianne Feinstein) (asking if it is possible to draft a single standardized document that would be accepted by all creditors and credit bureaus).

248. See *supra* notes 234-240 and accompanying text (describing the credit reporting agencies' failure to protect against fraudulent applications).

## IV. THE FTC RESPONSE TO IDENTITY THEFT

Congress and the federal government have not completely ignored the issue of identity theft and its effect on innocent victims.<sup>249</sup> On October 30, 1998, President Clinton signed the Identity Theft and Assumption Deterrence Act (“ITADA”) to address the growing problem of identity theft.<sup>250</sup> ITADA amends 18 U.S.C. § 1028 to make it a federal crime when anyone “knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity.”<sup>251</sup> While the criminal code previously addressed fraudulent documents, ITADA amended federal law to include the theft of identifying information.<sup>252</sup>

Significantly, ITADA recognizes the needs of victims of identity theft.<sup>253</sup> First, ITADA entitles victims to restitution.<sup>254</sup> Before ITADA, only the financial institution that recorded the loss was entitled to recovery and restitution,<sup>255</sup> the victim did not have legal standing<sup>256</sup>

---

249. See, e.g., H.R. 4311—*The Identity Theft Prevention Act of 2000: Hearing Before the House Comm. on Banking and Fin. Servs.*, 106th Cong. 3 (2000) (introducing a bill that would require credit bureaus to establish procedures to assist victims). See generally GAO REPORT, *supra* note 27 (studying the prevalence of identity theft); FTC, U.S. Government’s Central Website on Identity Theft (establishing a website, maintained by the FTC, providing information for consumers to prevent identity theft and assist those that are victimized), at <http://www.ftc.gov/idtheft> (last visited Aug. 3, 2002).

250. Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1028(a)(7) (2000)); see *May 20, 1998 Hearings*, *supra* note 8, at 13 (statement of James Bauer, Deputy Assistant Director, Office of Investigations of the U.S. Secret Service) (explaining that law enforcement officials consider enactment of ITADA to be “a proactive answer to what [was] being handled in a reactive manner”); Paul A. Greenberg, *Identity Fraud—The Great E-Commerce Roadblock*, ECOMMERCETIMES, July 12, 2001 (reporting that Lawrence William was the first person tried under ITADA after being charged with fourteen counts of identity fraud), available at <http://www.ecommercetimes.com/perl/story/11932.html> (last visited Aug. 10, 2002).

251. 18 U.S.C. § 1028(a)(7); see also *id.* § 1028(d)(3) (defining “means of identification” as including name, social security number, date of birth, driver’s license, or identification number).

252. See *May 20, 1998 Hearings*, *supra* note 8, at 13 (statement of James Bauer, Deputy Assistant Director, Office of Investigations of the U.S. Secret Service) (explaining before ITADA, “the predicate offense of stealing someone’s identity to create counterfeit and/or fictitious documents gained little or no attention” and “the focus had been on the ultimate criminal objective”).

253. See 144 CONG. REC. S9503 (daily ed. July 30, 1998) (statement of Sen. Jon Kyl) (arguing that ITADA recognizes the victim and the crime of identity theft while previous law did not).

254. S. REP. NO. 105-274, at 4 (1998); see also *May 20, 1998 Hearings*, *supra* note 8, at 21 n.47 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC) (explaining that ITADA grants consumer victims rights of restitution for costs incurred in clearing credit history, including civil or administrative proceedings that may occur).

255. See *May 20, 1998 Hearings*, *supra* note 8, at 20 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC)

and was entitled to no recovery.<sup>257</sup>

Second, ITADA authorizes the FTC to take a proactive role in assisting victims of identity theft.<sup>258</sup> Section 5 of ITADA directs the FTC to establish, not later than one year after the date of enactment, a Centralized Complaint and Consumer Education Service for Victims of Identity Theft.<sup>259</sup> In particular, ITADA commands the FTC to establish procedures to “log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief that one or more of their means of identification have been assumed, stolen or otherwise unlawfully acquired.”<sup>260</sup> ITADA also requires the FTC to provide informational materials to identity theft victims and to refer complaints to appropriate entities, including the three major credit bureaus and law enforcement.<sup>261</sup>

Interestingly, Congress gave the FTC a central role under ITADA, even though it is a civil agency with no criminal enforcement authority.<sup>262</sup> Because its mission is to promote consumer protection, the FTC, operating through the FTC Act,<sup>263</sup> is authorized to create

---

(explaining that before ITADA was enacted, the financial institution was considered the only victim); *see also* *United States v. Karro*, 257 F.3d 112, 121 (2d Cir. 2001) (holding that an upward departure in sentencing under ITADA was appropriate because of the nonmonetary harm to victims).

256. *See March 7, 2000 Hearings, supra* note 24, at 12 (statement of Maureen Mitchell, victim) (explaining that she and her husband were not treated as true victims, and could not sue until ITADA was passed).

257. *See* 143 CONG. REC. S2742 (daily ed. Mar. 21, 1997) (statement of Sen. Jon Kyl) (recounting story of Bob Hartle who spent over \$10,000 to clear his name but was unable to receive restitution for his expense).

258. *See* Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, § 5, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1028(a)(7) (2000)) (requiring the FTC to design a Centralized Complaint and Consumer Education Service for Victims of Identity Theft); 144 CONG. REC. S9503 (daily ed. July 30, 1998) (statement of Sen. Jon Kyl) (explaining that the FTC program provides “real time relief” to victims); *see also* GAO REPORT, *supra* note 27, at 2 (stating that before ITADA was enacted, no federal agency had overall jurisdiction regarding identity theft); Hoar, *supra* note 9, at \*3 (explaining how the Department of Justice, the FTC, and other agencies work together to prevent, investigate, and prosecute identity thieves).

259. Identity Theft and Assumption Deterrence Act § 5.

260. *Id.* § 5(a)(1).

261. *Id.* § 5(a)(2)-(3).

262. *See* Summary of Proceedings, National Summit on Identity Theft (Mar. 15-16, 2000) (explaining that the FTC is a civil agency that has been given the responsibility for identifying and preventing identity theft without criminal enforcement authority), *available at* <http://www.securityunit.com/other/natifoc.htm> (last visited Aug. 10, 2002); *see also* *March 7, 2000 Hearings, supra* note 24, at 34 n.20 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining most identity theft cases are addressed through criminal prosecution, but FTC only has civil authority).

263. Federal Trade Commission Act, 15 U.S.C. § 45(a) (2000); *see* *May 20, 1998 Hearings, supra* note 8, at 18 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC) (stating that the FTCA “provides

this Centralized Complaint and Consumer Education Service.<sup>264</sup> Additional statutes give the FTC authority to create and enforce rules relating to specific industries involved in identity theft, such as credit reporting agencies.<sup>265</sup> Because identity theft is integrally related to the credit industry and its control over identification materials, “examining the causes and consequences of identity theft and exploring potential solutions fall within the scope of the Commission’s mandate.”<sup>266</sup> Specifically, the FTC’s role is to assist victims and law enforcement by collecting and sharing information from public and private entities.<sup>267</sup>

A. *The FTC Initiatives under the Identity Theft and Assumption Deterrence Act*

To satisfy its obligations under ITADA, the FTC established three programs focusing on prevention, protection, and assisting victims.<sup>268</sup> The goal of the FTC programs is to act as an information clearinghouse that is designed to:

---

the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce”); *see also On Line Fraud: Are Consumers Safe?: Hearing Before the House Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Prot.*, 107th Cong. 20 (2001) [hereinafter *May 23, 2001 Hearings*] (statement of Eileen Harrington, Associate Director of Marketing Practices, FTC) (explaining the FTC’s jurisdiction over the entire economy, including the Internet, is unique because other federal agencies only have jurisdiction over specific markets or industries).

264. *See May 20, 1998 Hearings, supra* note 8, at 18 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC) (stating that the mission of the FTC is “to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by ensuring vigorous competition”).

265. *See, e.g., Fair Credit Reporting Act*, 15 U.S.C. §§ 1681–1681u (2000) (requiring credit bureaus to ensure accuracy of consumer credit reports by investigating disputed records and limiting disclosure of credit reports to only permissible purposes); *Fair Credit Billing Act*, 15 U.S.C. §§ 1666–1666j (2000) (requiring creditors to correct billing mistakes and limiting liability for unauthorized credit card use).

266. *See May 20, 1998 Hearings, supra* note 8, at 18 (statement of David Medine, Associate Director Credit Practices, Bureau of Consumer Protection, FTC) (explaining that FTC became involved in identity theft issues in 1996 when it conducted two public meetings); *see also April 22, 1999 Hearings, supra* note 22, at 20 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (commenting that “[a]s an outgrowth of its broader concern about financial privacy, the Commission has been involved in the issue of identity theft for some time”).

267. *See April 22, 1999 Hearings, supra* note 22, at 21–22 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining that the FTC will serve “as a central, federal source of information”).

268. *See id.* (outlining the components of (1) the toll-free telephone hotline, (2) the identity theft complaint database, and (3) consumer education materials); *see also MARCH 2001 DATA, supra* note 32, at 6 (describing programs established by FTC under ITADA).

1) support criminal law enforcement efforts by collecting data in one central database and making referrals as appropriate; 2) to provide consumers with information to help them prevent or minimize their risk of identity theft; 3) to streamline the resolution of the credit and financial difficulties consumers may have when they become victims of identity theft; and 4) to enable analysis of the extent of, and factors contributing to, identity theft in order to enrich policy discussions.<sup>269</sup>

1. *The identity theft hotline*

First, the FTC established an "identity theft hotline" on November 1, 1999.<sup>270</sup> The hotline, 1-877-ID-THEFT, is based on the success of the FTC's Consumer Response Center, a call center established in 1997 for general consumer complaints.<sup>271</sup> Consumers who report identity theft will speak to a counselor who will explain the process of resolving credit issues.<sup>272</sup>

Counselors tell victims to contact the credit reporting agencies, to obtain copies of their credit reports from each agency, and to request that a fraud alert be placed on their credit report.<sup>273</sup> The counselors also encourage the victim to call and write each creditor with whom the identity thief has opened an account.<sup>274</sup> Counselors are trained to explain to victims their rights under the FCRA and the Fair Credit Billing Act,<sup>275</sup> and they also advise the victims to file a police report.<sup>276</sup>

The identity theft hotline has been an important resource for consumer victims of identity theft.<sup>277</sup> At first, it was receiving approximately 445 calls per week.<sup>278</sup> By July 2000, the hotline had

---

269. *March 7, 2000 Hearings, supra* note 24, at 34 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC).

270. *See July 12, 2000 Hearings, supra* note 20, at 9-10 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (describing how the FTC's hotline assists victims, as well as consumers, with resolving and preventing identity theft).

271. *See April 22, 1999 Hearings, supra* note 22, at 22 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining that identity theft hotline will build on the success of the FTC's general purpose consumer hotline).

272. *See July 12, 2000 Hearings, supra* note 20, at 9-10 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (providing details of hotline and counselor responsibilities by outlining a victim's legal rights and responsibilities to identify, resolve, and prevent identity theft).

273. *See id.* at 10 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining that when a fraud alert appears on a credit report, the consumer will be notified every time a credit application is submitted).

274. *Id.*

275. *Id.*

276. *See id.* (stating that a police report is the best means of proving identity theft to a creditor).

277. *See generally* MARCH 2001 DATA, *supra* note 32 (summarizing the data collected from callers since the hotline was launched).

278. *Id.*

received 20,000 calls from potential and actual victims of identity theft.<sup>279</sup> By March 2001, the hotline was receiving over 2,000 calls per week.<sup>280</sup>

## 2. *The identity theft clearinghouse*

Second, the FTC implemented the Identity Theft Data Clearinghouse (“Clearinghouse”) to satisfy the FTC’s obligation to refer victims to appropriate entities.<sup>281</sup> The Clearinghouse acts as a “comprehensive, government-wide repository of information collected from victims of identity theft.”<sup>282</sup> Complaints and reports from victims are entered into the database when consumers speak to a counselor on the hotline.<sup>283</sup>

The Clearinghouse is designed to facilitate the communication between the FTC and other agencies involved in identity theft.<sup>284</sup> For example, Clearinghouse information is incorporated into the Consumer Sentinel Database, a secure website that forwards FTC information to law enforcement agencies.<sup>285</sup> Reviewing the information collected in the Clearinghouse database gives the FTC and law enforcement the means to identify and track patterns of identity theft<sup>286</sup> and to pinpoint specific practices that facilitate the

---

279. *July 12, 2000 Hearings, supra* note 20, at 9 n.5 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC).

280. MARCH 2001 DATA, *supra* note 30, at 2.

281. See Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, § 5(a)(3), 112 Stat. 3007, 3010 (1998) (providing that the FTC shall establish procedures to refer complaints to three consumer reporting agencies and law enforcement).

282. *March 7, 2000 Hearings, supra* note 24, at 35 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC).

283. See MARCH 2001 DATA, *supra* note 32, at 1 (showing that by March 2001, the Clearinghouse had been contacted by and recorded data for 45,593 actual victims of identity theft); see also FEDERAL TRADE COMMISSION, IDENTITY THEFT VICTIM COMPLAINT DATA: FIGURES AND TRENDS IN IDENTITY THEFT, NOVEMBER 1999 THROUGH MAY 2001 Figure 1 (2001) (reporting that by May 2001, the Clearinghouse had recorded almost 60,000 victims).

284. See, e.g., *ID Theft: Links and Publications* (listing government agencies involved with identity theft, including: Social Security Administration, Federal Bureau of Investigation, Department of Justice, and Secret Service), available at <http://www.consumer.gov/idtheft/info.htm> (last visited Aug. 8, 2002); see *April 22, 1999 Hearings, supra* note 22, at 22 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining that Clearinghouse provides a central database that enables many agencies “to share and manage data so as to more effectively track down identity thieves and assist consumers”).

285. See *July 12, 2000 Hearings, supra* note 20, at 11 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (stating that in July 2000, law enforcement agencies were given access to the Clearinghouse through their desktop computers); see also MARCH 2001 DATA, *supra* note 32, at 1 n.1 (noting that more than 1,000 law enforcement officers rely on Consumer Sentinel as an investigative resource).

286. See *July 12, 2000 Hearings, supra* note 20, at 11 (statement of Jodie Bernstein,

crime.<sup>287</sup> The FTC is also exploring ways to obtain and share information with other agencies, such as the Social Security Administration,<sup>288</sup> to further ease the burden on victims.<sup>289</sup> The FTC, however, is hesitant to share the Clearinghouse database information with private companies.<sup>290</sup> In an effort to control access to the personal information contained on the database and to reduce the risk of the database itself aiding the identity thieves, the FTC plans to limit private companies' access to the database.<sup>291</sup> Instead, the FTC will evaluate the data collected and forward only certain information to specific private industries involved in an identity theft pattern.<sup>292</sup>

### 3. Consumer education

Finally, to satisfy its obligation under ITADA, the FTC established a consumer education program.<sup>293</sup> The FTC began its education efforts by coordinating with public and private organizations that had been researching identity theft and methods of prevention.<sup>294</sup> In February 2000, the FTC issued a Consumer Alert that explained what

---

Director, Bureau of Consumer Protection, FTC) (stating that "[t]he FTC will continue to comb through the data to spot cases for referral, but has also enabled others to use the data to ferret out the bad actors.").

287. See *March 7, 2000 Hearings*, *supra* note 24, at 35 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (stating that "we will look at whether certain types of transactions or business practices lead to greater opportunities for the theft of a person's personal information or facilitate the misuse of that information once obtained.").

288. See *id.* at 36 (explaining that the database will begin including information obtained from the Social Security Administration because social security numbers are the means used to steal an identity).

289. See *April 22, 1999 Hearings*, *supra* note 22, at 22 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining that a call to one agency should simultaneously inform other agencies of identity theft because a victim of social security misuse should not have to call all related federal agencies to ensure that their complaint was handled by appropriate one).

290. See *July 12, 2000 Hearings*, *supra* note 20, at 11 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (claiming that "[t]he Commission does not envision providing access to the complete database for these private sector entities.").

291. See *id.* (stating that "[u]nfettered access could interfere with law enforcement efforts").

292. See *id.* (explaining that FTC data analysts will forward complaints to companies they find to be engaged in high risk business practices or are not responding to consumer complaints).

293. See Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, § 5(a)(2), 112 Stat. 3007, 3010 (1998) (requiring the FTC to establish procedures to "provide informational materials to individuals"); see also *April 22, 1999 Hearings*, *supra* note 22, at 22 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (outlining the FTC's initial plan of consumer education).

294. See *April 22, 1999 Hearings*, *supra* note 22, at 22 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining that the FTC is working with government and private groups "to develop unified, comprehensive consumer education materials for victims of identity theft").

consumers should do if they become victims of identity theft.<sup>295</sup> In February 2001, the FTC published a booklet, entitled *ID Theft: When Bad Things Happen to Your Good Name*.<sup>296</sup> The FTC also educates consumers through its Internet website, <http://www.consumer.gov/idtheft>.<sup>297</sup>

### B. *The FTC Successes*

By outlining the proper steps necessary to prevent additional fraud and to begin to clear a credit report, the FTC initiatives have eased some of the burden on consumer victims of identity theft caused by the credit industry.<sup>298</sup> For example, when the FTC began keeping data through its identity theft program, only approximately half of the victims who contacted the FTC had also informed one of the three credit bureaus, and only half had placed fraud alerts on their reports.<sup>299</sup> Less than half had contacted financial institutions.<sup>300</sup> Of these, only twelve percent had also sent written notification.<sup>301</sup> Finally, only fifty-three percent had contacted their police department.<sup>302</sup> The FTC “minimizes the risk of further harm” by encouraging victims to complete the process and to contact entities that they may not have known were involved, including credit bureaus and their local police department.<sup>303</sup>

### C. *The FTC Prevention Efforts*

The FTC also has made significant progress in protecting consumer privacy by limiting the credit reporting agencies’ ability to

---

295. See FTC Consumer Alert: Identity Crisis—What to Do If Your Identity Is Stolen (Feb. 2000) (describing steps for a victim to take to identify, resolve, and prevent identity theft), available at <http://www.consumer.gov/idtheft> (last visited Aug. 3, 2002).

296. See generally FTC, ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME (2001) (explaining general information on identity theft prevention).

297. See *July 12, 2000 Hearings*, supra note 20, at 10 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (stating that the website has received more than 108,000 hits since it was launched in November 1999).

298. See *March 7, 2000 Hearings*, supra note 24, at 13 (statement of Maureen Mitchell, victim) (explaining that information she received from the FTC was valuable because there were government bureaus she would not have known to notify).

299. See MARCH 2001 DATA, supra note 32, at 5 (reporting that only fifty-two percent of victims had notified any of the credit bureaus).

300. See *id.* (noting that forty-nine percent of victims had contacted the financial institutions involved).

301. *Id.*

302. *Id.*

303. See *id.* (reporting that the Hotline counselors explain what steps victims need to take to prevent further harm because many victims do not know what to do when their identity has been stolen).

disclose personal identifying information to third parties.<sup>304</sup> In *Trans Union Corp. v. FTC*,<sup>305</sup> Trans Union challenged an FTC order that defined target marketing lists as “consumer reports,”<sup>306</sup> which under the FCRA, would be prohibited from being sold for target marketing purposes.<sup>307</sup> Trans Union’s primary business is to collect information on individuals from financial institutions and lenders, compile credit reports, and sell the reports to third parties who extend credit.<sup>308</sup> Trans Union receives information from financial institutions in the form of “tradelines,” which include a customer’s name, address, social security number, account type, credit limit, and payment history.<sup>309</sup>

In 1987, Trans Union created its second product line, a target marketing service,<sup>310</sup> which relies on information stored on Trans Union’s main database.<sup>311</sup> Each person in the target marketing database has either two tradelines or one tradeline and a confirmed address.<sup>312</sup> The target marketing service generates mailing lists based on consumer information stored in its database.<sup>313</sup> Trans Union sells these lists to companies that solicit offers to people in certain classes.<sup>314</sup> The lists contain only names and addresses, but the

---

304. See *Trans Union Corp. v. FTC*, 245 F.3d 809, 811 (D.C. Cir. 2001) (banning the sale of target marketing lists because they qualify as “consumer reports,” which are prohibited under the FCRA); *Individual Reference Servs. Group, Inc. v. FTC*, 145 F. Supp. 2d 6, 13 (D.D.C. 2001), *aff’d sub nom. Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002) (holding that credit header information is subject to privacy regulations and the regulations promulgated by the FTC are lawful).

305. 245 F.3d 809 (D.C. Cir. 2001).

306. 15 U.S.C. § 1681a(d)(1) (2000). FCRA defines consumer report as:

any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for credit. . . .

*Id.*

307. See *Trans Union Corp.*, 245 F.3d at 814-16 (upholding the FTC order banning the sale of consumer report lists for target marketing purposes).

308. See *id.* at 812 (explaining that Trans Union receives 1.4 to 1.6 billion records per month and their database now contains information on 190 million adults).

309. *Id.*

310. See *Trans Union Corp. v. FTC*, 81 F.3d 228, 229 (D.C. Cir. 1996) (stating that Trans Union diversified and created TransMark, now Trans Union Lists).

311. See *Trans Union Corp.*, 245 F.3d at 812 (describing that MasterFile, the database used for the target marketing service, is a subset of Trans Union’s consumer credit database).

312. *Id.*

313. See *id.* (explaining that MasterFile uses information in its consumer credit database to compile lists of people who satisfy certain characteristics).

314. See *Trans Union Corp.*, 81 F.3d at 229 (explaining that Trans Union uses tradelines to generate a base list, from which it creates additional sub-lists, such as the “Urban Ethnics” or “EmptyNesters”).

purchasers know the characteristics of individuals because Trans Union sorts the database according to the characteristics a certain solicitor requests.<sup>315</sup>

To determine whether target marketing lists were “consumer reports” under the FCRA, the D.C. Circuit questioned whether the information “is used or expected to be used . . . for the purpose of serving as a factor in establishing the consumer’s eligibility for credit,” which is the definition of a consumer report.<sup>316</sup> Trans Union allows marketers to request lists based on credit limits, loan dates, number of tradelines, and the existence of tradelines.<sup>317</sup> The court found that the mere existence of a tradeline is a factor in credit granting decisions.<sup>318</sup> With this evidence, the court held that the tradeline information used in creating target marketing lists satisfied the second element of the definition of “consumer report.”<sup>319</sup> Therefore, the sale of target marketing lists was held impermissible under the FCRA.<sup>320</sup> This decision has a direct bearing on the prevention of identity theft.<sup>321</sup> With the restriction on target marketing, a consumer’s personal information is less accessible, decreasing the potential for misuse by identity thieves.<sup>322</sup>

More recently, consumer privacy advocates made another important stride in their mission to protect disclosure of personal information and to prevent identity theft.<sup>323</sup> In affirming the district court decision in *Individual Reference Services Group (“IRSG”) v. FTC*,<sup>324</sup> the D.C. Circuit held that all the information a credit reporting agency obtains and uses is subject to the new Gramm-Leach-Bliley

---

315. See *Trans Union Corp.*, 245 F.3d at 812 (explaining that purchasers of lists know that every individual on a list satisfies certain characteristics requested).

316. *Id.* at 813-14 (quoting 15 U.S.C. § 1681a(d)(1) (2000)).

317. See *id.* at 815 (stating that the information in these categories are used in prescreening and credit scoring models).

318. See *id.* at 816 (explaining that banks consider the existence of a tradeline as a factor in prescreening or credit models).

319. See *id.* at 814 (finding that Trans Union’s list contain information that “is used or expected to be used as a factor in establishing credit eligibility”).

320. See *id.* (affirming the FTC’s decision that target marketing lists are protected by the FCRA).

321. See *Ways and Means Hearings, supra* note 2, at 121 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (arguing that the *Trans Union* decision narrowed the ability for identity thieves to obtain information).

322. See *id.* at 121-22 (explaining that disclosing personal information led to information broker web sites that gave identity thieves easy access to information).

323. See Brian Krebs, *Court Decision Deals Another Blow to Credit Data Firms*, NEWSBYTES NEWS NETWORK, June 29, 2001 (reporting that the credit reporting industry will have to comply with new privacy rules), available at 2001 WL 23415895, at \*1.

324. 145 F. Supp. 2d 6 (D.D.C. 2001), *aff’d sub nom.* *Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002).

privacy rules.<sup>325</sup> In *Trans Union*, IRSG and Trans Union challenged the inclusion of “credit header” information in the privacy regulations implemented under the Gramm-Leach-Bliley Act (“GLB Act”).<sup>326</sup> Trans Union credit reports contain both identifying information and tradeline information obtained from financial institutions.<sup>327</sup> The identifying information, called the “credit header,” consists of a person’s name, address, social security number, and phone number.<sup>328</sup> Trans Union receives “credit header” information and sells it to businesses that use the information to detect fraud, enforce child support orders, and to locate individuals involved in financial crimes.<sup>329</sup>

Before the D.C. Circuit’s ruling, “credit header” information was not considered a consumer report and was not subject to the FCRA.<sup>330</sup> As a result, “credit header” information could be sold to third parties for any purpose.<sup>331</sup> Despite arguments that the “credit header” does not have a direct bearing on creditworthiness, the misappropriation of the basic personal information that is contained in the credit header caused the identity theft of Adelaide Andrews and many

---

325. *Trans Union LLC*, 295 F.3d at 48-50; see also Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. § 6801(2000)); 16 C.F.R. §§313.10-313.12 (2000) (mandating new privacy rules that limit the disclosure of nonpublic personal information by financial institutions, require financial institutions to give notice of their privacy policies, define conditions under which a third party can receive nonpublic personal information, and allow consumers to opt-out of sharing personal data kept by financial institutions).

326. See *Trans Union LLC*, 295 F.3d at 46 (arguing that the privacy regulations are unconstitutional and unlawful).

327. See *Individual Reference Servs. Group*, 145 F. Supp. 2d at 14.

328. *Id.* at 17; see also *Privacy Update: Exam Guidelines, Anti-Spam Bill, Credit Headers, ID Theft*, CBA REPORTS, June 1, 2001 (explaining that credit headers are based on credit reports but are stripped of financial content and distributed separately from credit reports), available at 2001 WL 11962810, at \*2.

329. See *Individual Reference Servs. Group*, 145 F. Supp. 2d at 14 (describing three Trans Union products that sell credit header data: Trace, ReTrace, and ID Search); see also Edmund Sanders, *Curb on Sale of Consumer Data Upheld*, L.A. TIMES, May 8, 2001, at C1 (quoting a Trans Union spokesman’s statement that the court’s decision will negatively affect the beneficial uses for selling “credit header” information, such as finding fugitives, runaways, and parents that owe child support).

330. See *Individual Reference Servs. Group*, 145 F. Supp. 2d at 17 (explaining that the FTC and the credit reporting agencies agree that “credit header” information was not protected by the FCRA).

331. See *id.* (explaining that “credit header” information was not subject to the FCRA because it was not thought to bear on credit worthiness); see also 15 U.S.C. § 1681b (2000) (prohibiting disclosure of information that is considered a consumer report, unless it is for a permissible purpose); *Ways and Means Hearings*, *supra* note 2, at 121 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (arguing that the credit header loophole “allowed credit bureaus to separate a consumer’s so-called header or identifying information from the balance of an otherwise strictly regulated credit report and sell it to anyone for any purpose”).

others.<sup>332</sup>

The GLB Act,<sup>333</sup> passed in November 1999, was intended to increase competition among firms in the financial services industry.<sup>334</sup> Because this increase in competition would lead to increased accessibility of personal information, the GLB Act required agencies to promulgate rules describing the conditions under which financial institutions could disclose “nonpublic personal information” to third parties.<sup>335</sup> The GLB Act defined “nonpublic personal information” as “personally identifiable financial information.”<sup>336</sup> The FTC final rule further defined “personally identifiable financial information” as “any information a consumer provides to a financial institution to obtain a financial product or service.”<sup>337</sup> According to the FTC, “credit header” information would be included in this definition because it is given to a credit reporting agency, which the FTC considered to be a financial institution.<sup>338</sup> Therefore, disclosure of “credit header” information would be subject to the same strict privacy rules as information obtained by other financial institutions.<sup>339</sup>

First, *Trans Union* asserted it was not a “financial institution” under the GLB Act.<sup>340</sup> Since the credit reporting services are “closely related to banking or managing or controlling banks,” the court held that the credit reporting agencies were “financial institutions” and the

---

332. See *Ways and Means Hearings*, *supra* note 2, at 122-24 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (stating that the availability of the social security number in credit header information has aided identity thieves and stalkers).

333. Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended at 15 U.S.C. § 6801 (2000)).

334. See *Trans Union LLC*, 295 F.3d at 46 (describing the purpose of the GLB Act); *Individual Reference Servs. Group*, 145 F. Supp. 2d at 17-18 (explaining that the purpose of the GLB Act is to provide a framework for financial services providers that will increase product availability to allow domestic providers to compete globally).

335. See *Individual Reference Servs. Group*, 145 F. Supp. 2d at 17-18 (describing that the Act balances consumer’s need for privacy and the desire to increase competition within the financial sector); see also 15 U.S.C. § 6802(a)-(b) (requiring financial institutions to give notice of privacy policies and allow a consumer to opt-out of disclosing their information).

336. 15 U.S.C. § 6809(4)(A) (2002).

337. 16 C.F.R. § 313.3(o)(1). See also *Individual Reference Servs. Group*, 145 F. Supp. 2d at 26 (explaining that the regulations fill the gap in the term’s definition).

338. See *Trans Union LLC*, 295 F.3d at 51 (holding that a credit reporting agency is a “financial institution” and explaining that the FTC’s interpretation of 15 U.S.C. § 6809(4)(A) includes *any* information provided by a customer to a financial institution).

339. See *Individual Reference Servs. Group*, 145 F. Supp. 2d at 26 (arguing that “credit header information is improperly subsumed within the ambit of the GLB Act.”).

340. See *id.* at 32; *Trans Union LLC*, 295 F.3d at 48 (arguing that the FTC had no authority over credit reporting agencies because they should not be considered “financial institutions” under the GLB Act).

FTC clearly had rulemaking authority over them.<sup>341</sup> Second, the consumer reporting agencies claimed the FTC's definition of "personally identifiable financial information" as "any information provided to [a financial institution] to obtain a financial service or product" conflicted with the plain language of the GLB Act.<sup>342</sup> They argued that information in a "credit header" is not considered "financial" according to the dictionary definition of that term.<sup>343</sup> Therefore, the FTC definition eliminates the "financial" component of "personally identifiable *financial* information" as defined in the statute.<sup>344</sup>

To determine whether the FTC definition was a reasonable interpretation of the statute, the court applied the two part test outlined in *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*<sup>345</sup> Under *Chevron*, the court examines whether Congress expressly addressed the question at issue.<sup>346</sup> The court is bound to give effect to congressional intent if it is clear from the statute or the legislative history.<sup>347</sup> However, if the statute is silent or the congressional intent is ambiguous, the court considers whether the agency's interpretation is a permissible construction of the statute.<sup>348</sup> According to *Chevron*, the court will give deference to a reasonable agency interpretation of an ambiguous statutory provision.<sup>349</sup>

Applying the *Chevron* test, the district court examined the language of the GLB Act, additional provisions of the GLB Act, and the legislative history.<sup>350</sup> The district court found that "nonpublic personal information" was meant to encompass a large list of information, based on the context in which it was received, "rather than the intrinsic nature of the information itself."<sup>351</sup> Although the

---

341. See *Trans Union LLC*, 295 F.3d at 48-9 (finding that a credit reporting agency fit the GLB Act's definition of "financial institution").

342. See *id.* at 51 (claiming that if the plain meaning of the statute were applied, only information related to a consumer's financial condition would be subject to the privacy rules); see also 16 C.F.R. § 313.3(o)(1)(i)-(iii) (defining "personal identifiable financial information").

343. See *Individual Reference Servs. Group*, 145 F. Supp. 2d at 26-7 (citing the dictionary definition of "financial" and arguing that credit header information should be removed from the GLB Act privacy rules because it is not "financial" information).

344. *Id.*

345. 467 U.S. 837, 842-43 (1984); *Trans Union LLC*, 295 F.3d at 51.

346. *Chevron*, 467 U.S. at 842-43.

347. *Id.*

348. *Id.*

349. *Id.*

350. See *Individual Reference Servs. Group*, 145 F. Supp. 2d at 26-29 (applying tools of statutory construction to the GLB Act to determine the definition of personally identifiable financial information).

351. *Id.* at 27.

legislative history suggested this included “credit header” data,<sup>352</sup> the district court characterized the definition as ambiguous.<sup>353</sup> Because the definition of “personal identifiable financial information” was ambiguous, the court would give deference to the agency’s definition, if it were reasonable.<sup>354</sup> The court held that the FTC had justified its inclusion of “credit header” information in its definition of nonpublic personal information when the FTC stated:

financial institutions rely on a broad range of information that they obtain about consumers, including information such as addresses and telephone numbers. . . . [I]t would be inappropriate to carve out certain items of information that a particular financial institution might rely on when providing a financial product or service.<sup>355</sup>

The district court concluded that the FTC’s interpretation was a reasonable construction of the statute; therefore, the inclusion of the “credit header” information in the GLB privacy regulations was justified.<sup>356</sup> The D.C. Circuit affirmed, emphasizing that the FTC’s definition of “personally identifiable financial information” was consistent with the broad definition of “financial institution” in the GLB Act.<sup>357</sup>

As a result of this decision, credit reporting agencies are unable to share “credit header” information because they do not give their customers notice of their sharing policies with respect to “credit header” information, or notice of the right to opt out of sharing.<sup>358</sup> Adelaide Andrews’ case illustrates that only basic information, like

---

352. *See id.* at 29 (reviewing congressional debates in which two members of Congress expressly included “credit header” information in the definition of personal financial information).

353. *See id.* (stating that “[t]his inclusion of credit header information within the meaning of ‘financial information’ during debates in both Houses of Congress reinforces the finding that the statute cannot be interpreted as argued by plaintiffs would like, but more fairly should be characterized as ambiguous with respect to that term.”).

354. *See id.* at 31 (explaining that under circumstances where Congress’ actions are ambiguous and where an agency shows its regulations were carefully and reasonably drafted, the court must defer to the agency’s interpretation of the statute).

355. *Id.*

356. *See id.* at 46 (finding that the regulations drafted by the FTC were lawful and do not breach the plain meaning of the GLB Act or constitute an improper construction of the statute).

357. *See Trans Union LLC*, 295 F.3d at 51 (reasoning that subjecting “credit header” information to the privacy rules would be consistent with the Act’s definition of “financial institution,” which encompasses activities that are not traditionally considered “financial”).

358. *See Ways and Means Hearings, supra* note 2, at 121 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (explaining that the decision will prevent identity theft, at least temporarily).

that included in a “credit header,” is needed to steal an identity.<sup>359</sup> With this decision, cases like *Adelaide Andrews*’ could be less frequent because the disclosure of one’s basic information would be restricted.<sup>360</sup>

These cases demonstrate the FTC’s commitment to preventing identity theft and protecting consumers from unwanted disclosure of their personal information.<sup>361</sup> The effect of the decision, however, is limited because credit reporting agencies could obtain the personal information from other institutions that are not regulated by the GLB Rules.<sup>362</sup> In addition, the “credit header” information is only protected until the financial institutions amend their privacy policies to provide notice of the possibility their information will be shared.<sup>363</sup> Finally, the restriction on disclosure of information does nothing to assist consumers who have already had their identities stolen and are burdened with the task of reestablishing their reputation.<sup>364</sup>

## V. POSSIBLE AGENCY AND LEGISLATIVE PROPOSALS

### A. *Voluntary Initiatives*

Victims of identity theft suggest that a uniform protocol of procedures would significantly alleviate the burden of restoring their names, reputations, and credit histories.<sup>365</sup> The FTC can use the tools

---

359. See generally *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (illustrating that a name and social security number are sufficient to successfully steal a victim’s identity).

360. See *Ways and Means Hearings*, *supra* note 2, at 121 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (explaining that the decision helps prevent identity theft, but the credit header loophole should also be closed by statute).

361. See *id.* (describing the two cases involving the FTC as “a strong victory for privacy protection”).

362. See Millett, *supra* note 242, at 13 (explaining that credit reporting agencies can still sell the same information, but they must obtain it from other sources).

363. See *Ways and Means Hearings*, *supra* note 2, at 121 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (stating that credit header data will only be protected until the financial institutions amend their privacy policies to give notice that it will be shared and then only those consumers that opt-out of sharing the information will be protected).

364. See Morphy, *supra* note 17 (describing the many obstacles an identity theft victim faces, such as the statute of limitations and the substantial length of time required to clear an erroneous credit report); see also Millett, *supra* note 242, at 12 (explaining that the procedure to clear a fraudulent credit history is “like a tennis match”).

365. See *March 7, 2000 Hearings*, *supra* note 24, at 21 (statement of Maureen Mitchell, victim) (recommending a “standardized, universally accepted national protocol for victims of Identity Theft to follow. The bona fide victim should have to fill out one set of documents containing a notarized affidavit, a police report, a notarized handwriting sample . . . to be able to submit copies to each merchant.”).

it has established to develop procedures to relieve some of the burdens that the credit industry created.<sup>366</sup> Specifically, the FTC referral service and its authority over identity theft issues can help streamline the procedures victims of identity theft must endure to regain financial health and rebuild their reputations.<sup>367</sup>

The FTC has debated two voluntary initiatives to facilitate a victim's process of rebuilding his credit and reputation.<sup>368</sup> First, the FTC drafted and recently published a uniform fraud declaration that all credit bureaus and all creditors would accept.<sup>369</sup> This standardized declaration form reduces the burden on the victims because they are no longer required to fill out multiple forms with the same information.<sup>370</sup> Standardizing the fraud notification process, however, raises a legitimate concern that the declaration could lead to more identity theft if it fell into a criminal's hands.<sup>371</sup>

Second, the FTC proposed the "one stop fraud alert" to streamline the fraud alert notification process.<sup>372</sup> The "one stop fraud alert" would allow the consumer to call one number to have a fraud alert placed on their credit report at all of the three credit bureaus,

---

366. See IDENTITY THEFT WORKSHOP, *supra* note 36, at 181 (remarks of Betsy Broder, Assistant Director, Division of Planning and Information, FTC) (explaining a legislative proposal where the FTC would take on the obligation of creating model protocols, if credit reporting agencies were unsuccessful).

367. See *March 7, 2000 Hearings*, *supra* note 24, at 38 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining the FTC is looking at ways to streamline the remediation process and citing the benefit to consumers of making a single phone call to have a fraud alert placed on all three credit reports, with a copy then mailed to their home).

368. See generally IDENTITY THEFT WORKSHOP, *supra* note 36 (discussing the "model fraud affidavit" and the "one stop fraud alert"); see also FTC, IDENTITY THEFT WORKSHOP: ONE STOP SHOP BREAKOUT SESSION 13 (Oct. 24, 2000) [hereinafter BREAKOUT SESSION] (remarks of Helen Foster, Attorney, Division of Planning and Information, FTC) (explaining FTC proposals are voluntary initiatives and not mandated by ITADA).

369. ID THEFT AFFIDAVIT, at <http://www.consumer.gov/idtheft/affidavit.htm> (last visited Aug. 4, 2002); see *March 7, 2000 Hearings*, *supra* note 24, at 47 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (responding to question from Sen. Dianne Feinstein, that "a standardized form is just one measure that would relieve the burden on identity theft victims").

370. See 147 CONG. REC. S9079 (daily ed. Sept. 4, 2001) (statement of Sen. Dianne Feinstein) (explaining that the new model form, which will be accepted by the three credit bureaus and many major financial institutions, will substantially decrease the paperwork burden on victims).

371. See IDENTITY THEFT WORKSHOP, *supra* note 36, at 249 (remarks of Steve Munson, Deputy Attorney General, State of New Jersey, Division of Criminal Justice) (proffering that a uniform fraud affidavit must be accompanied by a confidentiality guarantee if it is to be prevented from falling into the wrong hands).

372. See *March 7, 2000 Hearings*, *supra* note 24, at 47 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (explaining another way to streamline processes would be to reduce number of phone calls a victim had to make).

reducing the number of phone calls a victim must make.<sup>373</sup> The Associated Credit Bureaus, the trade association that represents the credit reporting agencies, has opposed the “one stop fraud alert,” claiming it will create problems with the consumer’s right, under the FCRA, to dispute records on credit reports.<sup>374</sup> Credit bureaus fear liability from consumers who are not made aware that the “one stop call” is only a first step.<sup>375</sup>

Nevertheless, victims agree that the ability to make a single phone call—rather than several—would alleviate some of their burden.<sup>376</sup> The FTC, rather than the credit reporting agencies, is the appropriate entity to establish a “one call” service.<sup>377</sup> While the FTC does not have access to the credit reporting agencies’ databases,<sup>378</sup> the tools it has established, such as the Hotline and the role it was given as a referral service, make it the most logical agency to establish the “one stop fraud alert” outside of the fraud dispute process.<sup>379</sup>

The credit reporting agencies have attempted to address the burden on identity theft victims through a series of voluntary initiatives.<sup>380</sup> In 1997, the agencies formed the Individual Reference

---

373. BREAKOUT SESSION, *supra* note 368, at 4-5 (remarks of Helen Foster, Attorney, Division of Planning and Information, FTC).

374. The Associated Credit Bureau has changed its name to Consumer Data Industry Association. See 15 U.S.C. § 1681i (2000) (explaining the dispute resolution process for records on credit reports); see also IDENTITY THEFT WORKSHOP, *supra* note 36, at 160-61 (remarks of Stuart Pratt, Vice President of Government Relations, Associates Credit Bureaus, Inc.) (stating that “you have begun triggering a series of duties we have under the law” and explaining how a “one stop fraud alert” outside of the dispute resolution process may be misleading for consumers who may think calling a single number will act as the dispute resolution process required under the FCRA).

375. See BREAKOUT SESSION, *supra* note 368, at 1 (remarks of Helen Foster, Attorney, Division of Planning and Information, FTC) (explaining that “one stop shop” terminology is misleading and FTC envisions a two step process where a fraud alert first is placed, and second, the credit reporting agencies are contacted); *id.* at 14 (remarks of Janine Benner, Consumer Associate, California Public Interest Research Group (“CALPIRG”)) (explaining that it should not be portrayed as a single number that will solve all identity theft problems).

376. See *id.* at 15 (remarks of Janine Benner, Consumer Associate, CALPIRG) (stating that one call would give “reassurance . . . that you do have the fraud alert on there before you start going through the other tasks”).

377. See IDENTITY THEFT WORKSHOP, *supra* note 36, at 103 (remarks of Helen Foster, Attorney, Division of Planning and Information, FTC) (explaining that because credit reporting agencies are competitors, they cannot share information in the same way as noncompetitors).

378. See BREAKOUT SESSION, *supra* note 368, at 21 (remarks of Phil McKee, Assistant Director, Internet Fraud Watch) (arguing that only way to make an outside phone number work is if the agency had access to credit reporting agencies’ databases, which is not currently possible).

379. See *id.* at 15 (remarks of Janine Benner, Consumer Associate, CALPIRG) (stating that the FTC can act as a facilitator in the process of contacting creditors and credit reporting agencies).

380. See July 12, 2000 Hearings, *supra* note 20, at 73-75 (statement of Stuart Pratt,

Services Group, which instituted self-regulatory principles for the credit industry.<sup>381</sup> Associated Credit Bureaus announced their own voluntary initiatives in March 2000.<sup>382</sup> Each credit reporting agency has also addressed identity theft in some way.<sup>383</sup> These voluntary initiatives, however, have been unsuccessful, as social security numbers and personal information are still being obtained by thieves.<sup>384</sup>

### B. Legislative Proposals

On October 4, 2001, Timothy Muris, the new Chairman of the FTC, announced that he would not pursue new privacy legislation.<sup>385</sup> Instead, he intends to increase the enforcement of existing privacy

---

Vice President of Government Relations, Associates Credit Bureaus, Inc.) (describing the ACB efforts to address fraud, including the creation of the Fraud and Security Task Force, fraud units, and enhanced customer service programs).

381. See *id.* at 65 (statement of Steven Emmert, Director of Government and Industry Affairs, Reed Elsevier Inc.) (describing that companies in the IRSG commit to restricting distribution of non-public information, educating the public about their databases, and acquiring non-public information from reputable sources).

382. See Press Release, Associated Credit Bureaus, Credit Reporting Industry Announces Identity Theft Initiatives (Mar. 14, 2000) (outlining six point program to improve identity theft assistance), available at <http://www.acb-credit.com/qspage.cfm?PageID=116> (last visited July 10, 2001); see also Rich, *supra* note 180, at A9 (explaining the credit bureaus' voluntary initiatives and their opposition to reform).

383. See, e.g., Press Release, Trans Union, From Hollywood to Main Street: Trans Union Helps Victims, Law Enforcement Ward Off Credit Fraud (June 18, 2001) (discussing Trans Union's Fraud Victim Assistance Department), available at <http://www.transunion.com/Press/PressReleaseDetails.jsp?id=/releases/press/data/2001061808331300.xml&page=4> (last visited Aug. 4, 2002); *Equifax Consumer Services* (advertising Credit Watch, which allows a consumer to have Equifax monitor your credit report for a fee), available at <http://www.econsumer.equifax.com> (last visited Aug. 4, 2002). See generally EXPERIAN, AN EXPERIAN WHITE PAPER: LIFTING THE LID OFF IDENTITY THEFT AND TRANSACTION FRAUD 8 (2002) (discussing Experian's products that detect fraud).

384. See Rich, *supra* note 180, at A9 (reporting that FTC supported new legislation because the self regulatory approach was inadequate and resulted in few changes); see also *Ways and Means Hearings*, *supra* note 2, at 122 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (explaining that IRSG initiatives to restrict access to social security numbers were unsuccessful because social security numbers can still be purchased on websites).

385. See Timothy Muris, Remarks at The Privacy 2001 Conference (Oct. 4, 2001) (stating that "[a]t this time, we need more law enforcement, not new laws."), available at <http://www.ftc.gov/speeches/muris/privisp1002.htm> (last visited Aug. 8, 2002); Erika Morphy, *FTC Shifts Internet Privacy Stance*, ECOMMERCE TIMES, Oct. 5, 2001 (noting that the FTC's new position on privacy is a reversal of the FTC position on privacy under the Clinton Administration), available at <http://www.ecommercetimes.com/perl/story/13969.html> (last visited July 23, 2002); see also K. Daniel Glover, *Which Way Internet Privacy?*, FIN. EXECUTIVE, July/Aug. 2001, at 24 ("[P]rivacy lacks a 'champion' in either the Bush administration or Congress."); Jonathan Krim, *FTC Will Not Seek New Privacy Laws*, WASH. POST, Oct. 5, 2001, at E11 (reporting that opponents believe that the new policy ignores five years of studies that show new legislation is necessary).

laws.<sup>386</sup> However, aggressive legislative action requiring the credit industry to establish more efficient procedures for victims of identity theft, and creating an incentive to follow those procedures, is essential to make a real impact on a victim's remediation process.<sup>387</sup> The FTC's voluntary initiatives, while alleviating some of the burden on a victim of identity theft, do not hold the credit industry accountable for its role in the identity theft problem.<sup>388</sup>

1. *Legislation to hold the credit industry accountable*

Most of the pending legislation to prevent identity theft limits the display of the social security number.<sup>389</sup> Other pieces of legislation call for the credit header loophole to be closed by statute.<sup>390</sup> While prevention is vital, legislation should also impose an obligation on the credit industry to establish procedures that facilitate the process of restoring a victim's credit history and penalize the industry for failing to do so.<sup>391</sup>

In 2000, Sen. Dianne Feinstein (D-Cal) introduced the Identity Theft Prevention Act of 2000<sup>392</sup> as an attempt to empower victims by addressing the shortcomings of the credit industry and implementing measures to help victims recover.<sup>393</sup> The bill restricted the

---

386. See Morphy, *supra* note 385 (reporting that the FTC plans to increase its enforcement budget by fifty percent).

387. See *July 12, 2000 Hearings, supra* note 20, at 35 (statement of Beth Givens, Director, Privacy Rights Clearinghouse) (explaining that laws are needed to create incentives for the credit industry to change how it operates).

388. See *March 7, 2000 Hearings, supra* note 24, at 38 (statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC) (discussing state legislation that is aimed at directly assisting victims); 146 CONG. REC. E587 (daily ed. Apr. 13, 2000) (statement of Hon. Darlene Hooley) (advocating for legislation that would impose fines on creditors for not following procedures to protect privacy).

389. See, e.g., Social Security Number Misuse Prevention Act, S. 848, 107th Cong. (2001) (prohibiting the sale of a social security number without holder's consent); Identity Theft Protection Act, H.R. 220, 107th Cong. (2001) (prohibiting federal or local agencies from requesting or requiring disclosure of social security numbers or mandating a national identification number).

390. See, e.g., Social Security Number Privacy and The Identity Theft Prevention Act of 2001, H.R. 2036, S. 1014, 107th Cong. (2001) (restricting sale of social security numbers and subjecting the credit header information to the FCRA); Personal Information Privacy Act of 2001, H.R. 1478, 107th Cong. (2001) (redefining "consumer report" in the FCRA to exclude identifying information in a local telephone book so as to ensure credit header information is kept confidential); see also *Ways and Means Hearings, supra* note 2, at 118 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (advocating that legislation close the credit header loophole).

391. See, e.g., The Identity Theft Prevention Act of 2000, H.R. 4311, 106th Cong. (2000) (codifying the fraud alert process and imposing fines on the credit industry for not recognizing fraud alerts).

392. Identity Theft Prevention Act of 2000, S. 2328, 106th Cong. (2000).

393. See 146 CONG. REC. S1987 (daily ed. Mar. 30, 2000) (statement of Sen. Dianne Feinstein) (seeking to empower victims because they are often treated like

distribution of identifying information, thereby addressing the plight of an identity theft victim.<sup>394</sup> It also required credit reporting agencies to investigate discrepancies in a person's account<sup>395</sup> and to notify all creditors of a change of address to alert them of possible suspicious activity.<sup>396</sup> Most significantly, Senate Bill 2328 also increased the FTC's authority, allowing the agency to impose fines on creditors that ignore a fraud alert.<sup>397</sup> Finally, the bill called on the credit industry to develop model forms and procedures to be used by consumers to inform the credit industry of identity fraud.<sup>398</sup>

In 2001, Senator Feinstein introduced a similar bill, the Identity Theft Prevention Act of 2001,<sup>399</sup> which prevents identity theft and assists victims in restoring their reputations.<sup>400</sup> This bill recognizes the inadequacies of the current system for identity theft victims and endorses the uniform reporting protocol debated by the FTC.<sup>401</sup> It also requires credit card machines to truncate credit card numbers and to notify consumers when an additional credit card is requested on an existing account.<sup>402</sup> The bill requires credit bureaus to notify

---

criminals).

394. *See id.* (explaining that S. 2328 closes a loophole in FCRA that allows personal identifying information to be marketed and only sold by allowing disclosure for permissible purposes).

395. *See* S. 2328 § 5 (directing the FTC to devise regulations requiring consumer reporting agencies to investigate discrepancies between the information a consumer provides and the information already on file).

396. *See id.* § 3 (requiring credit reporting agencies to submit notification of fraud when a new address is used on an application for credit); *see also* 146 CONG. REC. S1987 (statement of Sen. Dianne Feinstein) (explaining that the bill improves how credit card companies monitor requests for new cards and changes of address because this would alert consumers of potential fraud).

397. *See* S. 2328 § 4 (requiring creditors to comply with fraud alert procedures); *see also* 146 CONG. REC. S1987 (statement of Sen. Dianne Feinstein) (discussing that the bill would give the FTC authority to impose fines on creditors that ignore a fraud alert).

398. *See* S. 2328 § 10 (directing FTC to establish model forms and standard procedures, which will assist aggrieved consumers in reporting incidents of identity theft); *see also* 146 CONG. REC. S1987 (statement of Sen. Dianne Feinstein) (explaining that if the credit industry fails to implement measures to assist victims in notifying creditors of fraud, the FTC can take action).

399. S. 1399, 107th Cong. (2001).

400. *See* 147 CONG. REC. S9078 (daily ed. Sept. 4, 2001) (statement of Sen. Dianne Feinstein) (introducing simple, practical proposals to help victims restore their financial reputations, and including provisions to make identity theft more difficult).

401. S. 1399 § 2(9)-(10). The Bill states that:

(9) [T]he resources available to identity theft victims are inadequate and both private sector and federal agencies should provide better and more sympathetic assistance to such victims; and (10) credit reporting agencies and issuers of credit should have uniform reporting requirements and effective fraud alerts to assist identity theft victims in repairing and protecting their credit.

*Id.*

402. *See id.* § 4 (providing that no person shall print more than the last five digits

creditors of discrepancies between the applicant's address and the address filed with the reporting agency.<sup>403</sup> In addition, to assist victims, the bill codifies the fraud alert process.<sup>404</sup> Senate Bill 1399 requires a credit reporting agency to include a fraud alert upon a customer's request and to notify creditors of the fraud.<sup>405</sup> Most importantly, creditors that fail to comply with a fraud alert will be penalized,<sup>406</sup> and the FTC is authorized to impose fines against creditors who ignore a fraud alert.<sup>407</sup>

More recently, the Restore Your Identity Act of 2001,<sup>408</sup> introduced in the Senate, also recognized the difficulties victims encounter and the responsibility the credit reporting agencies have in mitigating the harm that identity theft causes.<sup>409</sup> This bill alleviates the burdens victims face with creditors by requiring a business entity that possesses information on an identity theft to disclose that information within ten days of a request from the victim.<sup>410</sup> This provision provides an incentive for creditors to respond quickly to victims, reduces the time that it takes a victim to ascertain what has transpired, and prevents further harm.<sup>411</sup> The bill also recognizes the standardized fraud affidavit as a legitimate piece of identification.<sup>412</sup> Finally, the bill amends the FCRA to include a provision to block information that results from an identity theft, which would prevent further victimization by collection agencies.<sup>413</sup> Both Senate Bills 1399 and 1742 are important bills because they include measures to prevent

---

of a credit card number on any receipt); *see also* 147 CONG. REC. S9078 (statement of Sen. Dianne Feinstein) (explaining that truncating credit card numbers would prevent identity thieves from gaining information and account numbers from discarded receipts).

403. *See* S. 1399 § 3(b) (mandating a card issuer to notify a cardholder at both new and old address when an additional card is ordered and a change of address is submitted).

404. *See id.* (requiring credit reporting agencies to use fraud alerts and imposing penalties for not complying).

405. S. 1399 § 3(h)(1)-(2).

406. *Id.* § 3(h)(3).

407. 147 CONG. REC. S9078 (statement of Sen. Dianne Feinstein).

408. S. 1742, 107th Cong. (2001).

409. *See* S. 1742 § 2(6)-(9) (describing the harm victims face and the responsibility of the credit reporting agencies in assisting victims to clear the fraudulent reports and rebuild their credit).

410. *Id.* § 5(a)(1).

411. *See, e.g., Ways and Means Hearings, supra* note 2, at 14 (statement of Emeke Moneme, victim) (discussing the numerous difficulties she encountered in contacting creditors in a timely fashion, and stating that by the time she had completed contacting all the credit reporting agencies, a total of \$30,000 in credit had been used).

412. *See* S. 1742 § 5(c) (allowing the victim to provide the business entity with a police report and standardized fraud affidavit as proof of a fraud victim).

413. *See id.* § 6(e) (requiring that a credit reporting agency block information identified by the victim so that it cannot be reported).

identity theft and address the burdens victims face by including provisions to combat the “endless cycle of victimization” caused by the credit industry.<sup>414</sup>

## 2. *Legislation to amend the Fair Credit Reporting Act*

The legislative proposals that would have the most significant impact on victims of identity theft would amend the FCRA to incorporate an injury discovery rule.<sup>415</sup> As Justice Scalia stated in his concurrence in the *TRW* decision, “[t]hese cries, however, are properly directed not to us, but to Congress, whose job it is to decide how ‘humane’ legislation should be.”<sup>416</sup> Even if their statutory construction argument is correct, the Supreme Court’s conclusion that the FCRA does not cover an area of the law that “cries out” for an application of the injury discovery rule ignores the prevalence of identity theft and the degree of harm it can cause.<sup>417</sup>

Significantly, Senator Patrick Leahy (D-VT) recently introduced a bill that would make the FCRA more “humane.”<sup>418</sup> The adoption of an injury discovery rule, proposed in Leahy’s legislation and the corresponding House bill, would serve important public policy goals and reinforce the FCRA’s initial purpose to maintain accuracy of credit reports.<sup>419</sup> First, applying an injury discovery rule to the FCRA would provide an incentive for credit reporting agencies to keep accurate data and to help stop identity thieves.<sup>420</sup> By refusing to

---

414. See 147 CONG. REC. S9078 (daily ed. Sept. 4, 2001) (statement of Sen. Dianne Feinstein) (describing that S. 1399 helps victims restore their credit histories quickly and makes it easier to report fraud).

415. See *Borrowers Beware*, *supra* note 44, at 6 (reporting that Congress should reconsider the needs of the identity theft victim and extend the discovery rule to cover more than suits that allege damages from misrepresentation of an FCRA violation).

416. *TRW, Inc. v. Andrews*, 534 U.S. 19, 38 (2001) (Scalia, J., concurring).

417. See *Borrowers Beware*, *supra* note 44, at 6 (urging Congress to “reconsider the balance between the needs of victims of identity theft and the need for repose by the credit reporting agencies”).

418. See Protect Victims of Identity Theft Act of 2001, S. 1723, H.R. 3368, 107th Cong. (2001) (introducing a bill to amend the FCRA to provide that an action can be brought for damages not later than two years after the date on which the violation is discovered or should have been discovered through reasonable diligence); see also 147 CONG. REC. S12,006 (daily ed. Nov. 16, 2001) (statement of Sen. Patrick Leahy) (stating that adopting the discovery rule in the FCRA “ensures that consumers have a fair chance to vindicate their rights”).

419. See *Editorial On Credit*, LAS VEGAS REV. J., Nov. 14, 2001, at 8B (outlining the need for incentives for the credit industry and noting that without the protection of the short two year statute of limitation, the credit reporting agencies themselves would be more likely to actively ensure the accuracy of their data).

420. See *id.* (reporting that the Supreme Court decision removes the incentive for credit reporting agencies to implement effective safeguards); see also 147 CONG. REC. S12,006 (statement of Sen. Patrick Leahy) (stating that S. 1723 would give the FCRA “real teeth to fulfill its mission of protecting the accuracy and privacy of consumer

extend an injury discovery rule beyond cases in which there is misrepresentation, the Supreme Court has enabled the credit reporting agencies to avoid liability for many claims.<sup>421</sup> If the statute were extended and the discovery rule applied, credit reporting agencies would be exposed to more liability and would maintain consumer records more carefully.<sup>422</sup>

TRW argued, however, that this exposure to liability would increase the “risk of litigating stale claims.”<sup>423</sup> The discovery rule, according to TRW, would “upset the balance” between the public’s interest in protecting claims and the defendant’s interest in finding repose.<sup>424</sup> TRW argued that the increased exposure to liability would create uncertainty for credit reporting agencies and would increase the cost of doing business by requiring the credit reporting agencies to retain files for a longer period of time.<sup>425</sup> Allowing defendants to contemplate a timeframe for liability is certainly a legitimate objective; however, TRW’s arguments in support of more timely repose are inadequate.<sup>426</sup> To support this assertion, TRW again relied on the notice and access provisions of the FCRA to prove that existing statutory provisions already adequately protect valid claims.<sup>427</sup> However, as explained above, these provisions are insufficient to protect valid claims.<sup>428</sup> In addition, considering the technology that is available to store massive amounts of data, the increase in the cost of doing business would be less severe than the credit industry

---

credit information”).

421. See 147 CONG. REC. S12,006 (statement of Sen. Patrick Leahy) (explaining that the statute of limitations could expire before a consumer suspects that their information has fallen into a criminal’s hands, thereby benefiting the credit reporting agencies).

422. See *Editorial On Credit*, *supra* note 419, at 8B (explaining that a longer statute of limitations would encourage credit reporting agencies to actively monitor the accuracy of the reports they compile); see also 147 CONG. REC. S12,006 (statement of Sen. Patrick Leahy) (stating that the legislation would encourage credit bureaus to establish procedures to prevent identity theft).

423. Petitioner’s Brief at 30, *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (No. 00-1045).

424. See *id.* (stating that “application of the discovery rule tips the balance struck by a statute of limitations in favor of protecting claims and against repose”).

425. See *id.* at 28-30 (stating that the industry maintains files on nearly 200 million consumers and since they are updated monthly, the burden on credit reporting agencies would be significant).

426. See Respondent’s Brief at 40-47, *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (No. 00-1045) (undercutting TRW’s arguments and arguing that TRW overstates the consumer benefits of the FCRA “notice” and “access” provisions).

427. See Petitioner’s Brief at 31, *TRW* (No. 00-1045) (arguing that the FCRA requires consumers to be notified of any adverse action taken against them).

428. See *supra* notes 173-76 and accompanying text (describing the inadequacies of the notice and access provisions).

anticipates.<sup>429</sup>

Second, an injury discovery rule would provide a mechanism for monitoring the credit reporting agencies.<sup>430</sup> With the statute of limitations beginning at the time of the violation, there is virtually no monitor over the industry.<sup>431</sup> Although the FTC has authority to enforce the FCRA, its resources are limited and the task is overwhelming.<sup>432</sup> As advocates of consumer privacy have indicated, credit reporting agencies lack sufficient incentive to ensure privacy and accuracy because their primary clients are creditors.<sup>433</sup> The credit grantors themselves also have no incentive to bring an action under the FCRA because they can absorb losses associated with it.<sup>434</sup>

Only the victims of identity theft have an incentive to enforce the FCRA.<sup>435</sup> Recognizing that accuracy of credit reports is vital to the health of the economy, Congress amended the FCRA to include a private right of action for damages as an enforcement mechanism.<sup>436</sup> Compliance with the FCRA, therefore, depends in large part on these private actions.<sup>437</sup> The Supreme Court's application of a violation occurrence rule, however, eliminates this civil remedy that the FCRA was intended to create, leaving the credit reporting agencies with little regulation.<sup>438</sup>

---

429. See Brief of Amici Curiae the National Association of Consumer Advocates et al. at 18, *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (No. 00-1045) (arguing that personal data is the business, not the burden of the credit reporting industry).

430. See Brief for the United States and the Federal Trade Commission as Amici Curiae Supporting Respondent at 24-25, *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (No. 00-1045) (advancing the argument that the public interest purposes of the FCRA can only be achieved by use of a discovery rule).

431. See Brief of Amici Curiae the National Association of Consumer Advocates et al. at 19-20, *TRW* (No. 00-1045) (explaining how the credit reporting agencies are virtually unregulated and noting that it would take an army of regulators to review the millions of files maintained by the three major credit reporting agencies).

432. See Brief for the United States and the Federal Trade Commission as Amici Curiae Supporting Respondent at 28, *TRW* (No. 00-1045) (explaining that because of the enormous volume of consumer reports issued every year, the FTC simply does not have the resources to monitor credit reporting agencies effectively).

433. Brief of Amici Curiae the National Association of Consumer Advocates et al. at 19-20, *TRW* (No. 00-1045).

434. *Id.*

435. *Id.*

436. See *id.* at 5-6 (explaining that the FCRA was enacted to regulate the credit industry because accuracy and privacy of credit reports is vital to a healthy banking system).

437. See *id.* at 20 (stating that the FCRA "was designed to be largely self enforcing").

438. See *id.* at 21 ("[I]f petitioner's position is sustained, the consumer reporting industry will be permitted to conduct its business, as it has been, with virtually no concern about possible private enforcement of its statutory duties relating to identity theft, so long as it can keep the victimized consumer in the dark for up to two years.").

## CONCLUSION

Identity theft is becoming an epidemic. Recently, identity theft accounted for more than forty percent of consumer fraud complaints.<sup>439</sup> The emotional, financial, and physical impact on victims is devastating.<sup>440</sup> The burdens that the recent Supreme Court decision creates and the current inadequacies in the credit reporting industry lead consumers to “cry out” for a reform of the legal and procedural assistance available for identity theft victims.<sup>441</sup> The FTC has taken an aggressive approach in meeting its obligations under ITADA and assisting victims.<sup>442</sup> However, it will not be until legislation addresses the “humanity” of the FCRA and creates an incentive for the credit industry to shore up its procedures and business practices, that victims will be able to fully reclaim their identities.<sup>443</sup>

---

439. *See Identity Theft Topped List of Fraud Complaints Filed By Consumers Last Year*, ST. LOUIS POST-DISPATCH, Jan. 24, 2002, at A10 (reporting on the FTC’s findings that the average identity theft victim incurs over \$1,000 rectifying the damage caused by identity thieves).

440. *See supra* note 142 and accompanying text (reporting that identity theft violates its victims and leaves lasting emotional, physical, and financial scars).

441. *See supra* notes 140-247 and accompanying text (arguing that a discovery rule triggering the statute of limitations and more consistent and responsible credit reporting procedures are necessary to ease the burden of a victim of identity theft).

442. *See supra* notes 268-97 and accompanying text (describing the programs established by the FTC designed to prevent identity theft and assist the identity theft victim).

443. *See supra* notes 389-438 and accompanying text (surveying recent legislative proposals designed to better protect victims and make credit reporting agencies more accountable).