



**ELECTRONIC PRIVACY INFORMATION CENTER**

---

Testimony and Statement for the Record of  
Chris Hoofnagle  
Deputy Counsel  
Electronic Privacy Information Center

Legislative Hearing on H.R. 2622,  
The Fair and Accurate Credit Transactions Act of 2003

Before the  
Committee on Financial Services,  
United States House of Representatives

July 9, 2003  
2128 Rayburn House Office Building

Chairman Oxley, Ranking Member Frank, and Members of the Committee, thank you for extending the opportunity to testify today on H.R. 2622, the Fair and Accurate Credit Transactions Act of 2003.

My name is Chris Hoofnagle and I am deputy counsel with the Electronic Privacy Information Center (EPIC), a not-for-profit research organization based in Washington, D.C. Founded in 1994, EPIC seeks to promote personal privacy rights and expand access to government information. The Fair Credit Reporting Act (FCRA) is a primary concern of EPIC, as it sets a legislative framework of Fair Information Practices to address rights and responsibilities in the handling of personal information. We maintain a web page on FCRA online at <http://www.epic.org/privacy/fcra/>.

The Privacy Rights Clearinghouse, Junkbusters Corp., Computer Professionals for Social Responsibility, Privacy Times, and Consumer Action have joined this written statement. The Privacy Rights Clearinghouse is a nonprofit consumer information and advocacy program. It offers consumers a unique opportunity to learn how to protect their personal privacy. Junkbusters Corp. is a privacy advocacy firm that helps people get rid of junk messages of all kinds: spam, telemarketing calls, unwanted junk mail, junk faxes, and more. CPSR is a public-interest alliance of computer scientists and others concerned about the impact of computer technology on society. Privacy Times Privacy is a leading subscription-only newsletter covering privacy. Evan Hendricks, a FCRA expert, has edited it since 1981. Consumer Action is a non-profit, membership-based organization founded 1971 that serves consumers nationwide by advancing consumer rights, referring consumers to complaint-handling agencies, advocating for consumers in the media and before lawmakers, and comparing prices on credit cards, bank accounts, and long distance services.

Today, we urge the Committee to strengthen protections in the FCRA. The record developed by the series of hearings held by the House Financial Services Committee and the Senate Committee on Banking, Housing, and Urban Affairs makes it clear that Americans need greater protections to address problems with identity theft, privacy, and inaccuracy. The hearing record also reflects the need to address affiliate information sharing, the link between information sharing and identity theft, the challenges that identity theft victims face, consumer awareness of information practices, medical information appearing on reports, the ease of access to Social Security Numbers, the problem of fly-by-night background investigation companies, credit scoring, and incomplete reporting practices that drive down credit scores.

We believe that the FCRA can be amended to address these problems. Accordingly, we make the following recommendations:

- Congress should not handcuff state legislators by preempting state law.
- Substantive privacy protections should be added to the FCRA to protect individuals against identity theft.
- Individuals need substantive improvements in the system to minimize inaccuracies, and to improve the correction process.
- Congress should ensure that medical information is not disclosed on credit reports.

- Congress should preserve the application of the FCRA to the background screening process.

While we commend Representatives Bachus, Hooley, Biggert, and Moore for introducing H.R. 2622, we believe that the bill does not fully address these needs. Our testimony below recommends substantive changes to the bill to address the risks to individuals as a result of shortcomings in the FCRA.

## **Brief History of the FCRA**

The FCRA, Public Law No. 91-508, was enacted in 1970 to promote accuracy, fairness, and the privacy of personal information assembled by Credit Reporting Agencies (CRAs).<sup>1</sup> CRAs assemble reports on individuals for businesses, including credit card companies, banks, employers, landlords, and others. The FCRA provides important protections for credit reports, consumer investigatory reports, and employment background checks.

The FCRA establishes rights and responsibilities for "consumers," "furnishers," and "users" of credit reports. Consumers are individuals. Furnishers are entities that send information to CRAs regarding creditworthiness in the normal course of business. Users of credit reports are entities that request a report to evaluate a consumer for some purpose.

The FCRA is a complex statute that has been significantly altered since 1970 by Congress and the courts. The Act's primary protection requires that CRAs follow "reasonable procedures" to protect the confidentiality, accuracy, and relevance of credit information. To do so, the FCRA establishes a framework of Fair Information Practices for personal information that include rights of data quality (right to access and correct), data security, use limitations, requirements for data destruction, notice, user participation (consent), and accountability.

The FCRA was passed to address a growing credit reporting industry in the United States that compiled "consumer credit reports" and "investigative consumer reports" on individuals. The FCRA was the first federal law to regulate the use of personal information by private businesses.

The first major credit reporting agency, Retail Credit Co, was started in 1899. Over the years, Retail Credit purchased smaller CRAs and expanded its business into selling reports to insurers and employers.<sup>2</sup> By the 1960s, significant controversy surrounded the CRAs because their reports were sometimes used to deny services and opportunities, and individuals had no right to see what was in their file.<sup>3</sup>

By the late 1960s, there was abuse in the industry, including requirements that investigators fill quotas of negative information on data subjects. To do this, some investigators fabricated

---

<sup>1</sup> 15 U.S.C. § 1681, available at <http://www.ftc.gov/os/statutes/fcra.htm>.

<sup>2</sup> Alan F. Westin, *PRIVACY AND FREEDOM* (Athenum 1967). "...the largest American private investigative agency, the Retail Credit Company, which rates persons for a wide variety of purposes including industrial security, has 7,000 investigators, maintains dossiers on forty-two million people, and grosses more than \$100 million annually from its activities."

<sup>3</sup> Robert Ellis Smith, *BEN FRANKLIN'S WEB SITE, PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET* (Privacy Journal, 2000).

negative information, others included incomplete information. Additionally, the investigators were collecting "lifestyle" information on data subjects, including their sexual orientation, marital situation, drinking habits, and cleanliness. The CRAs were maintaining outdated information, and in some cases, providing the file to law enforcement and to unauthorized persons. Public exposure of the industry resulted in Congressional inquiry and federal regulation of CRAs.<sup>4</sup>

Years of legislative leadership by Representative Leonor Sullivan and Senator William Proxmire resulted in the passage of the FCRA in 1970. After its passage, Senator Proxmire attempted to broaden the FCRA's protections over the next ten years. Shortly the FCRA took effect on April 25, 1971, CRAs were pursued for violations of numerous provisions of the Act. Most recently, in January 2000, the three CRAs paid \$2.5 million in a case settlement brought by the FTC.

The most comprehensive amendments to the FCRA were contained in the Consumer Credit Reporting Reform Act of 1996 (P.L. 104-208). The Amendments contained a number of improvements to the FCRA, but it also included provisions that allow affiliate sharing of credit reports, "prescreening" of credit reports (unsolicited offers of credit made to certain consumers), and limited preemption of stronger state laws on credit.

The FCRA, like many other privacy statutes, provides a federal baseline of protections for individuals. The FCRA is only partially preemptive, meaning that except in a few narrow circumstances, state legislatures may pass laws to supplement the protections made by the FCRA. For instance, some states have passed laws requiring the CRAs to provide reduced cost, or free credit reports.

In a number of important areas state legislation is preempted until January 1, 2004.<sup>5</sup> After that date, states may enact stronger laws on prescreening (what constitutes a "firm offer" of credit, rules for opting out of receiving prescreened offers of credit), compliance duties (time in which a CRA must respond to reports of inaccuracies), user duties (notice and other requirements when a credit report is used for an adverse action), content of reports (length of time negative information can appear on the report), the duties of furnishers (accuracy of information provided, correction duties, notice of closed or disputed accounts), affiliate sharing, and the disclosures that CRAs must make to consumers.

In 1996, when the most recent amendments to the FCRA passed, certain state laws were grandfathered in, and not preempted by the federal law. Stricter laws exist on affiliate sharing (Vermont) and on duties of furnishers (California and Massachusetts).

### **Congress Should Not Handcuff State Legislators by Preempting State Law**

Section 101 of H.R. 2622 would extend preemption in the FCRA permanently. We believe that Congress should not extend the limited preemption in the FCRA beyond January 1, 2004. Consumers will lose important opportunities if preemption is extended—a continued federal ceiling will prevent states from creating additional needed protections. In our system of

---

<sup>4</sup> *Id.*

<sup>5</sup> 15 U.S.C. § 1681t.

government, preemption should only be used in limited situations, and generally, preemption is not appropriate for consumer protection legislation. Accordingly, we recommend that the Committee remove Section 101 in its entirety.

### *Historically Most Privacy Law Allows States to Provide Greater Protections*

In privacy and consumer protection law, federal ceiling preemption is an aberration. Historically, federal privacy laws have not preempted stronger state protections or enforcement efforts. Federal consumer protection and privacy laws, as a general matter, operate as regulatory baselines and do not prevent states from enacting and enforcing stronger state statutes. The Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Driver's Privacy Protection Act, and the Gramm-Leach-Bliley Act all allow states to craft protections that exceed federal law.<sup>6</sup>

Although the federal government has enacted privacy laws, most privacy legislation in the United States is enacted at the state level. Many states have privacy legislation on employment privacy (drug testing, background checks, employment records), Social Security Numbers, video rental data, credit reporting, cable television records, arrest and conviction records, student records, tax records, wiretapping, video surveillance, identity theft, library records, financial records, insurance records, privileges (relationships between individuals that entitle communications to privacy), and medical records.

The National Association of Attorneys General Privacy Subcommittee has also argued that the states have a traditional role in regulating privacy:

Congress should not preempt the states from enacting laws to safeguard and protect consumer privacy. The states' longstanding ability to enforce consumers' rights and prevent abuse, through enactment of substantive standards and by enforcement of existing state laws prohibiting unfair or deceptive acts, must be preserved. Consumer protection has traditionally been an area where the states' power to ensure fair competition and informed consumer choice has been preserved, not eliminated. This structure has worked well for many years and no need to alter it in the area of privacy has been demonstrated. Preemption of state law will only undermine consumer confidence in their dealings with the financial institutions, e-tailers and other on and offline businesses. This conclusion is especially powerful with respect to financial information, where Congress has already recognized the utility of privacy protections enacted at the state level.<sup>7</sup>

There is a presumption in American law that state and local governments are primarily responsible for matters of health and safety. *Hillsborough County v. Automated Medical Laboratories*, 471 U.S. 707 (1985) (there is a "presumption that state or local regulation of

---

<sup>6</sup> Respectively at 18 U.S.C. § 2510 et. seq., 12 U.S.C. § 3401, 47 USC § 551(g), 18 USC § 2710(f), 29 USC § 2009, 47 USC § 227(e), 18 U.S.C. § 2721, and Pub. L. No. 106-102, §§ 507, 524 (1999).

<sup>7</sup> NAAG Privacy Subcommittee Report: Privacy Principles and Background, National Association of Attorneys General, at <http://www.naag.org/naag/resolutions/subreport.php>.

matters related to health and safety is not invalidated under the Supremacy Clause"). Privacy is included in the category of health and safety issues as an area of regulation historically left to the states. For instance, in *Hill v. Colorado*, the Supreme Court upheld a law protecting the privacy and autonomy of individuals seeking medical care, as the law was intended to serve the "traditional exercise of the States' 'police power to protect the health and safety of their citizens.'" 530 U.S. 703 (2000).

*Preemption Stops States From Performing In Their Traditional Role as "Laboratories of Democracy"*

"It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."

--*New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

States enjoy a unique perspective that allows them to craft innovative programs to protect consumers. State legislatures are closer to their constituents and the entities they regulate. They are the first to see trends and problems, and are well-suited to address new challenges and opportunities that arise from evolving technologies and business practices.

An entire appendix to the 1977 Report of the Privacy Protection Study Commission was devoted to "Privacy Law in the States." This portion of the report speaks strongly to the value of state privacy protection:

Through constitutional, statutory, and common law protections, and through independent studies, the 50 States have taken steps to protect the privacy interests of individuals in many different types of records that others maintain about them. More often than not, actions taken by State legislatures, and by State courts, have been more innovative and far reaching than similar actions at the Federal level...the States have also shown an acute appreciation of the need to balance privacy interests against other social values.<sup>8</sup>

The report concludes:

This volume [the appendix to the 1977 report] underscores the central role the States can play as protectors of personal privacy and, more broadly, individual liberty...The States have demonstrated that they can, and do, provide conditions for experiments that preserve and enhance the interests of the individual in our technological, information-dependent society.<sup>9</sup>

State lawmakers have expressed similar observations about the role of diverse decision making authority. As North Carolina State Representative Dan Blue has argued:

---

<sup>8</sup> Privacy Law in the States, Appendix 1 to The Report of The Privacy Protection Study Commission Report, Personal Privacy in an Information Society, Jul. 1977.

<sup>9</sup> *Id.*

Federal preemption of state and local law presents a very serious challenge to our constitutional system of federalism...One of the advantages of federalism is that allows for greater responsiveness and innovation through local self-government. State and local legislatures are accessible to every citizen. They work quickly to address problems identified by constituents. The large number of state and local legislatures encourages innovation. A new policy is tested in one jurisdiction. If it works, other jurisdictions try it. If a mistake is made, it can quickly be corrected. But, if the policy jurisdiction of a state or locality has been preempted, then it cannot respond and it cannot innovate.<sup>10</sup>

*State Legislators Can Address New, Emerging Problems in the Credit System More Quickly Than Congress*

There is a particular danger that preemption of state enforcement authority will leave individuals with no remedies to privacy violations. In the states, attorneys general are elected, and thus have direct pressure from constituents to enforce consumer protection laws. Since the federal attorney general and agency officials are appointed, there is a risk that they will be less accountable to the public as political appointees.

EPIC Executive Director Marc Rotenberg has testified before Congress that one risk of federal ceiling preemption is that federal regulators may not be as responsive to individuals' problems:

As a general matter preemption is inconsistent with the structure of privacy law in the United States, and similar proposals have often killed important efforts to enact privacy legislation. But it is a particularly bad idea in this context where the FTC [Federal Trade Commission] would have so much control over the establishment of regulation as well as the provision of safe harbor status. Inadequate regulations or inattention to industry practices by the FTC could not be remedied by state or local authorities. States must retain the right to develop new safeguards to protect the interests of their citizens.<sup>11</sup>

North Carolina State Representative Dan Blue argues a similar position:

Federal regulatory agencies are not always successful in their mission of protecting the public. Moreover, over the past twenty years there has been something of an abdication by the federal government in such fields as consumer, environmental, and public health and safety protection. And, federal regulation, is often sluggish, bogged down in the elaborate federal administrative process and able to respond only slowly to the demands of the public. Federal agencies, in

---

<sup>10</sup> Statement of State Representative Dan Blue, Jr., President of the National Conference of State Legislatures, Before the Committee on Governmental Affairs Of the United States Senate, Regarding Federalism and Preemption of State Law, May 5, 1999, at <http://www.ncsl.org/statefed/bluefed.htm>.

<sup>11</sup> Testimony of Marc Rotenberg (PDF), *Hearing on S. 809, The Online Privacy Protection Act of 1999*, before the Subcommittee on Communications Committee on Commerce, Science and Transportation U.S. Senate, July 27, 1999, at [http://www.epic.org/privacy/internet/EPIC\\_testimony\\_799.pdf](http://www.epic.org/privacy/internet/EPIC_testimony_799.pdf)

other words, frequently are surpassed in performance by state officials who often can act quickly and effectively to protect their citizens.

States can act more quickly and aggressively because the structure of state administrative law is simpler and allows for swift decision-making. Also, state regulators are often more responsive to public opinion. For example, in most states, a popularly elected Attorney General is responsible for enforcement of antitrust, environmental, and consumer protection laws. State agencies, especially when they work cooperatively, also may have more law enforcement resources than comparable federal agencies. I would point in particular to the effectiveness of cooperative efforts of state attorneys general in addressing public health, consumer protection, and antitrust issues.<sup>12</sup>

### *Appeals to Efficiency In Nationally-Uniform Laws Are Specious*

The current credit reporting system has thrived under a federal baseline of protections that is supplemented by dozens of stronger state credit reporting laws. This country does not operate under a single, uniform standard for credit reporting. States have passed stronger laws in the areas of:<sup>13</sup>

- Arrest, Conviction, and Bankruptcy Records.
  - California: CRAs may not report bankruptcies after ten years. Cal. Civil Code 1785.13.
  - Massachusetts: CRAs may not maintain arrest records more than seven years old. Mass. Gen. Laws Ann. Ch. 93 § 52.
  - New Mexico, Kansas, and Montana: Criminal data must be purged from the report after seven years, bankruptcies must be purged after 14. N.M. Stat. Ann. § 56-3-6; Kan. Stat. Ann. §§ 50-704; Mont. Code Ann. §§ 31-3-112.
- Cost of Reports.
  - Georgia: Individuals are entitled to two free credit reports from each national credit reporting agency. Ga. Code Ann. § 10-1-393.
  - Colorado, Maryland, Massachusetts, New Jersey, and Vermont: Individuals are entitled to a free credit report once a year. Col. Rev. Stat. 12-14.3-105; Md. Comm. Law Code Ann. § 14-1209; Mass. Gen. Laws Ann. Ch. 93 § 59; N.J. Stat. Ann. 56:11-37; 9 Vt. Stat. Ann § 2480c.
  - Connecticut: Credit reports are \$5. Conn. Gen. Stat. Ann. § 36a-699a.
  - Minnesota: Caps the cost of credit reports at \$3. Minn. Stat. § 13C.01.
  - Maine: Caps the cost of credit reports at \$2. 10 M.R.S. § 1316.
- Credit Scores.
  - California: CRAs must furnish credit scores to individuals for a reasonable fee. Cal. Civil Code 1785.15.1.

---

<sup>12</sup> Statement of State Representative Dan Blue, Jr., President of the National Conference of State Legislatures, Before the Committee on Governmental Affairs Of the United States Senate, Regarding Federalism and Preemption of State Law, May 5, 1999, at <http://www.ncsl.org/statefed/bluefed.htm>.

<sup>13</sup> The citations and summaries of state laws verified were as of May 2003 and were drawn from Robert Ellis Smith, *Compilation of State and Federal Privacy Laws*, Privacy Journal 2002.



- Colorado: CRAs must provide a credit score to the consumer if one is used when extending credit secured by a dwelling. Colo. Rev. Stat. § 12-14.3-104.3.
  - Connecticut: Consumers must receive report within five days of receipt of the request; report must include all information in the file, including any credit score. Conn. Gen. Stat. § 36a-696.
  - Idaho: Prohibits insurers from raising rates, denying coverage, or canceling a policy primarily based on a credit rating or credit history. Idaho Code § 41-1843.
- Duties on Furnishers of Reports.
  - Massachusetts: Furnishers must follow reasonable procedures to ensure that the information reported to a CRA is accurate and complete, and furnishers may not provide information to a CRA if there is knowledge of or reasonable cause to believe such information is not accurate or complete. Mass. Gen. Laws Ann. Ch. 93 § 54A(a).
  - California: A person shall not furnish information on a specific transaction or experience to any consumer credit reporting agency if the person knows or should know the information is incomplete or inaccurate. Cal. Civil Code 1785.25(a).
- Duties on Users of Reports.
  - California: Individuals may receive a free copy of their credit report when it is requested by an employer. Cal. Civil Code 1785.20.5.
  - Utah: Credit grantors must notify consumers when negative information is furnished to a CRA. Utah Code Ann. 70C-7-107.
- Investigative Consumer Reports.
  - Arizona: Sources of investigative consumer reports must be furnished to the individual upon request. Ariz. Stat. § 44-1693(A)(4).
  - California: Investigative consumer reporting agencies must allow individuals to visually inspect files. Employers must furnish copies of the report to employees. Cal. Civil Code 1786.
- Notice to Consumers.
  - Colorado: CRAs must notify individuals where there have been eight inquiries on the report within one year or where adverse information is added to the report. Col. Rev. Stat. § 12-14.3-104.
- Sale of Personal Information:
  - California: Credit card issuers must give notice and an opportunity to opt-out when they sell customer information. Cal. Civil Code 1748.12 (c)(3)(b).
  - Connecticut: Selling the names from credit card purchases is prohibited. Conn. Gen. Stat. Ann § 42-133gg.
  - Maryland: It is illegal to disclose ATM or credit card numbers. Md. Crim. Code § 8-214.
  - Vermont: Credit reports can only be used for purposes consented to by the customer, and cannot be used for affiliate sharing without consent. Vt. Stat. Ann. § 2480e.
- Use of Medical Information.
  - Florida: An individual must be informed when genetic information was used to deny an opportunity. Fla. Stat. Ann. § 760.40(b).

Especially in the financial services and credit reporting areas, there has been an argument that a national ceiling of laws is needed in order to prevent "balkanization" or a "patchwork" of state laws. In fact, as the list above illustrates, many states currently have credit reporting laws that increase protections for consumers, and reduce the costs for access to consumer credit reports.

As the National Association of Attorneys General Privacy Subcommittee has argued:

Many businesses...argue the importance of a single, federal standard by citing the need for uniformity. They assert that a "patchwork" of state laws will make compliance costly and may stifle the development of markets both on and offline. In fact, businesses have long accommodated themselves to a range of state consumer protection statutes while maintaining a profitable enterprise. Courts have, for years, engaged in a process of reconciling potentially or actually conflicting laws through application of established legal principles to various factual situations. Such a tailored response is especially appropriate with respect to evolving technologies and new applications of those technologies. This flexible approach accommodates the needs of both businesses and consumers, while preserving state sovereignty in an area where states have traditionally had a significant role.<sup>14</sup>

*The Same New Technologies That Have Enabled Profiling Could Enable Compliance With Different State Laws*

Information, more than any other product, can be tailored with technology in order to comply with state requirements. In fact, the same companies lobbying for a uniform state standard for credit reporting already classify consumers into dozens of categories from "blue blood estates" to "hard scrabble" farmers. Technology has given these companies to discriminate among individuals who live on the same block; it can also enable these companies to comply with different state requirements on credit. There has never been a better time to experiment with this approach.

**Substantive privacy protections should be added to the FCRA to protect individuals against identity theft.**

Good privacy protections can help immunize individuals against identity theft. We recommend that the Committee analyze how individuals can be put in greater control of their personal information in order to prevent identity theft.

We think that the provisions in Title II of H.R. 2622 need to be strengthened in order to prevent identity theft. Specifically, Section 201 requires credit card issuers to engage in some due diligence when an application is made for an extra card at a different address. This provision is limited to existing card holders, that is, it does not apply to new applications for credit. Unfortunately this provision will provide little protection to consumers unless it applies to all applications for credit. The Committee should amend section 201 to require notice to the old and

---

<sup>14</sup> NAAG Privacy Subcommittee Report: Privacy Principles and Background, National Association of Attorneys General, at <http://www.naag.org/naag/resolutions/subreport.php>.

new addresses whenever an application for credit is made that does not match the address that is on file at the CRA.

Section 202 creates an important protection for victims of identity theft—the ability to place a fraud alert on a credit report and prevent credit issuers from starting new accounts. However, this fraud alert does not apply to check services and deposit account information service companies. The protections of Section 202 should apply to these entities, as recovering from forged or stolen check fraud is far more difficult than credit card fraud.

Section 205 provides for blocking of information resulting from identity theft. This section too has loopholes that largely invalidate the protections. First of all, the CRA does not have to block the information until 30 days after receiving the police report of the victim. Resellers of credit reports and check services are exempt as well. This exemption actually weakens existing law.<sup>15</sup>

Access to copies of the credit report is critical for victims of identity theft, but Section 501 of H.R. 2622 weakens such access. Section 501 provides that consumers can receive a free report once a year. However, the language eliminates free reports for victims of identity theft, the poor, and the unemployed. If this bill becomes law, identity theft victims, in particular, will lose because they will have to pay for numerous reports as they recover from the crime. This section would be improved significantly if free access for victims, the poor, and the unemployed were preserved. We further recommend that victims of identity theft be provided free credit monitoring service.

Beth Givens of the Privacy Rights Clearinghouse recommends two simple steps to eliminate the majority of identity theft: First, credit grantors must spend more time evaluating applicants before issuing credit. If just a short time—perhaps even just two more minutes—was spent evaluating information on the credit application, a significant amount of identity theft could be prevented. Credit grantors regularly issue credit to identity thieves who leave obvious errors on the application. Identity thieves often apply for credit under a different address than the victim, use incorrect dates of birth, use fabricated mothers' maiden names, or a different phone number than the victim.

For example, in one instance, an identity thief applied for a credit card at Dillard's Department Store using her own name and address, and the victim's social security number.<sup>16</sup> The thief's first initial and last name were the same as the victim's. Trans Union provided Dillard's with the victim's credit report because the first initial, last name, and social security number on the application matched their credit report file.<sup>17</sup> Dillard's approved the credit card, and the thief was issued a credit card under the victims' identity. If Dillard's were required to actually match information on the application fully with information from the CRA, this incident would have been prevented.

---

<sup>15</sup> See *FTC v. Credco*, File No. 95-23267 (1995).

<sup>16</sup> Erin Shoudt, *Comment. Identity theft: victims "cry out" for reform*, 52 Am. U. L. Rev. 339, 346-7 (2002)(citing *Andrews v. Trans Union Corp.*, 7 F. Supp. 2d 1056 (C. D. Cal. 1998)).

<sup>17</sup> *Id.* at 347.

California has adopted a sensible approach to manage this problem. California Civil Code 1785.14 requires CRAs to match three categories of identifying information from the file with the individual's application. The Committee has the opportunity to strengthen this protection by requiring that four information items from the application match the report. This simple, common-sense approach is likely to deter a significant amount of identity theft.

Ms. Givens' second recommendation is to require the CRAs to notify individuals when suspicious activity appears on the report. Such activity includes multiple inquiries in a short period of time (for instance, six new applications for credit within one month), or when negative information is furnished to the CRA. Either of these instances should result in notice to the individual. That notice would place the consumer on alert, and allow proactive steps to address the potential fraud. Colorado has enacted § 12-14.3-104 to address this situation. That section of the code requires a notice to the consumer where eight credit inquiries are made within a year or when negative information is furnished to the CRA. The Committee should adopt similar language that is stronger than the Colorado statute.

#### *The Committee Should Incorporate Measures to Protect the SSN*

Enacting stronger controls on the Social Security Number (SSN) is essential to curbing identity theft, but H.R. 2622 contains no such provisions. We recommend that the Committee visit the Social Security Number Privacy and Identity Theft Protection Act of 2001, 107 H.R. 2036, as a guide to limiting the use of the SSN. The measure was sponsored by Representative Clay Shaw (R-FL). In the 107th Congress, the bill enjoyed bi-partisan sponsorship of over 70 Members. The measure contained a comprehensive set of rights to protect individuals from identity theft.

Title I of the bill would have established important protections against public-sector sale or display of SSNs. These provisions would prohibit the display of the SSN on checks and government-issued employment cards. The bill would have prohibited disclosure of the SSN to inmates, and appearance of the SSN in public records. Increasingly, public records are a source for the collection of personal identifiers that then can be reused for any purpose.

The bill would have also prohibited "coercive disclosure" of the SSN—the practice of denying a product or service when an individual refuses to give a SSN. Additionally, Section 203 of that bill would have placed the SSN "below the line" on credit reports. This is an important and much needed protection that would stem trafficking in SSNs.

#### **Individuals need substantive improvements in the system to minimize inaccuracies, and to improve the correction process**

H.R. 2622 does not provide substantial improvements for consumers that will minimize inaccuracies or improve the correction process. Title III's only improvement is language that would allow notice of a dispute to be delivered to a reseller.

Section 401 of H.R. 2622 requires a CRA to notify the requestor when there is a discrepancy in addresses between the application and the report. However, this section hinges on the determination that the address be "substantially different," and notice to the consumer is not

required. It seems that when there is an application for credit on an individual's file with an inaccurate address, the consumer should receive notice too.

We believe that Section 402 is a good step forward. That section prohibits the furnishing of information that occurred because of fraudulent activity.

Section 403 would require notice to users of fraud where their assignees or agents learn of fraudulent activity on a report. Clearly this section should provide for notice to the CRA and to the consumer when evidence of fraud is discovered.

In summary, Titles III and IV of H.R. 2622 do not substantially improve the process. These titles do not recognize the importance of credit reports in consumers' lives, or the subtleties of the problems inherent in the system. We explain these problems below and make recommendations for improvements to the FCRA.

### *CRA's receive many complaints*

Our credit reporting system has serious flaws. On average, Experian's consumer center has received twenty five to thirty thousand consumer disputes or pieces of mail per day. Sometimes the figures are much higher, and the majority of the pieces of mail are actual disputes.<sup>18</sup> Likewise, CRA call centers receive large volumes of calls from consumers complaining about their credit reports on a daily basis. For example, CSC Credit Services receives 1500 to 2500 disputes per day.<sup>19</sup>

Because CRA's are the agencies that generate and manage credit reports, consumers have to trust CRA's to diligently follow-up on their complaints and resolve their disputes. The ability for consumers to review the accuracy of their credit reports is inhibited by two problems. The first is that consumers must pay to access their own credit reports. Only a few states require CRA's to provide consumers with their own reports without paying fees. Second, when consumers do get access to their credit reports, they do not receive the full credit reports, which are reserved for subscribers only. Subscribers get more detailed information about delinquencies, bankruptcies, etc. They get a risk score or a Fair Isaac score. As well as a banner where it says how much is delinquent, how many days total accounts are past due, how many derogatory items there are on the credit report, etc.<sup>20</sup>

*Perverse incentives pervade the system because dispute resolution is a cost center; subscriber business is a profit center.*

Ultimately, CRA's make money from their subscribers, not consumers. One former employee of Experian explained, "It is made clear that they [subscribers] pay your paycheck and don't forget it."<sup>21</sup> To a CRA, individuals are not the customers, they are data subjects: subscribers are the customers. As such, CRA's are motivated to cater to their subscribers. Individuals, however, are

---

<sup>18</sup> Deposition of Vicky Thompson 39:12-16, 40:3 (on file with EPIC).

<sup>19</sup> *Mendoza v. Experian*, No. 02-2465 (S.D. Tx. 2003)(Deposition of Janice Fogleman 0094:3-7).

<sup>20</sup> Deposition of Vicky Thompson 32:19-33:25 (on file with EPIC).

<sup>21</sup> *Id* at 56:23-57:1.

not a sufficient source of income to CRAs. As such, the consumer dispute resolution process is a cost center, and CRAs have little incentive to invest in resolving customer complaints. This problem translates into inadequate customer support. The less a CRA spends on complaint management, the lower their bottom line.

As noted above, CRAs receive vast amounts of complaints in a day. Yet, they do not provide adequate resources to handle these complaints. As a result, CRAs impose increasingly larger call handling quotas on their customer service representatives. One representative at Experian explained that when she began working at Experian, they were required to handle 62 calls per day, but within a couple of years, the quotas had increased to 100 complaint calls per day, leaving them only an average of 3-4 minutes per call.<sup>22</sup> The quotas are strictly enforced, and representatives can lose their jobs for failing to handle an adequate number of daily calls.<sup>23</sup> It is obvious that, in this environment, CRAs are not able to adequately address complaints. For example, representatives are specifically told not to prolong calls by asking questions of the callers, which discourages customer service representatives from taking initiative when try to resolve customer disputes.<sup>24</sup> For example, the following conversation from deposition of a CRA customer service representative is telling:

Q. So the quicker they can get the consumer off the phone, the better, regardless if they help them or not?

A. Exactly. I've seen reps transfer [consumers] to the main number. I've seen reps tell them, you know, call back or send in your proof to us and we'll dispute it that way. I mean, the reps weren't all—not everyone was willing to help.<sup>25</sup>

Because subscribers provide income to CRAs but consumers only burden the CRAs, there is a bias in favor of subscribers. This bias fosters an anti-consumer culture within CRAs, which is indoctrinated into new customer service representatives early on. In particular, during training, customer service representatives are specifically taught to mistrust consumers.<sup>26</sup> Moreover, one customer service representative explained that Experian's call center would block an individuals' number who called too many times.<sup>27</sup>

The pressures to reduce costs, and thus reduce service to consumers, is tremendous. For example, at one time, it was common for customer service representatives to resolve disputes by having conference calls between the consumers and subscriber. However, CRAs later began telling their representatives to do separate calls. Then finally, the CRAs began telling them not to call subscribers at all, as this was both time consuming and endangered upsetting the subscribers.<sup>28</sup>

*CRAs don't monitor furnishers and subscribers*

---

<sup>22</sup> *Id.* at 20:5-11

<sup>23</sup> *Id.* at 25:16-26:2.

<sup>24</sup> *Id.* at 24, 16-8.

<sup>25</sup> *Id.* at 71

<sup>26</sup> *Id.* at 26:3-19.

<sup>27</sup> *Id.* at 46:24-47:11.

<sup>28</sup> *Id.* at 21:21-22:09.

To some degree, CRAs act as conduits between subscribers, furnishers, and consumers. Because of this, they are in a particularly good position to monitor each of the parties. For example, CRAs could monitor subscribers so that they can see if there are a large number of fraud cases associated with a particular subscriber. Moreover, a CRA could monitor furnishers to see who might routinely report inaccurate information. However, not all CRAs keep these kinds of metrics. CSC Credit Services, for example, does not keep these metrics.<sup>29</sup>

*Factors that lead to bad data quality: CRAs are concerned more with quantity than quality*

CRAs are more concerned with amassing a large quantity of information about an individual because this is what the subscribers demand. This practice compromises data quality. For example, when retrieving information about an individual, CRA algorithms are designed to discard minor differences that occur in identifiers, such as incorrect digits in a social security number. The presumption here is that it is better to gather more information and have it be wrong than to risk excluding information. The potential resulting problem is a mixed file, where CRAs combine information from different individuals into one file. Victims of mixed files find it extremely difficult to correct this problem.

*Public records problem*

Sometimes, errors occur when CRAs incorrectly copy information from public records. CRAs generally rely on sub-vendors to supply them with information from public records. These public records usually do not have uniquely identifiable information, and as a result, CRAs may attribute incorrect information to individuals.

*Consumers Need Changes to the System to Ensure Accuracy*

Accuracy would be improved in the act if CRAs and furnishers were held to higher reinvestigation standards. The FCRA should be amended to require CRAs and furnishers to "conduct a reasonable reinvestigation to determine whether the disputed information is incomplete, inaccurate or unverifiable."

We recommend that the Committee maintain voluntary reporting, but require that furnishers that report aide by a "completeness" standard to prevent gaming the credit scoring system.

Further, the Committee should require that users provide to consumers any reports they rely on in making an adverse determination.

Finally, we recommend that consumers have a right of action against any furnisher who continues to provide inaccurate information to the CRA after notice is given that the information is inaccurate.

**Congress should ensure that medical information is not disclosed on credit reports**

---

<sup>29</sup> *Mendoza v. Experian*, No. 02-2465 (S.D. Tx. 2003)(Deposition of Janice Fogleman 0097:16-21, 0098:17-20).

Congress established a strong standard for the inclusion of medical information in credit reports. Under the Act, medical information should only appear in the report when it is provided directly from a health provider and the patient has consented to the transfer.<sup>30</sup>

A December 2002 study by the Consumer Federation of America and the National Credit Reporting Association, and a 2003 report of the Federal Reserve highlighted an emerging problem for consumers: despite the protections in the FCRA, some types of medical conditions or treatment can be inferred from items on credit reports.<sup>31</sup> Both studies found that the names of medical creditors could indicate what categories of treatment a consumer received. The current protections of the Act do not cover this loophole, and therefore Congress should correct this problem.

Furthermore, certain factors have exacerbated the problem caused by this loophole. The first is that medical collections commonly appear in credit reports, which exposes personal medical information to any person or business which requests a credit report. The Federal Reserve report found that 52 percent of collection actions are associated with medical bills.<sup>32</sup> Most of these collection items, however, are for small amounts. Sixty-six percent of medical collections are for amounts under \$250.<sup>33</sup> Second, medical organizations are beginning to use more aggressive collections techniques.<sup>34</sup> Mounting evidence suggests that health care providers are more vigorously pursuing consumers because insurance companies frequently reject or dispute claims.<sup>35</sup> Even if the insurer ultimately pays the claim, a collections item will remain on the consumer's report for seven years. To remove the collections item, the consumer must prove that it was a factual error.

The consequences of this confluence of problems are serious. Individuals' privacy is not adequately protected under the law. Additionally, the Access Project found that providers treat patients with medical collections differently—these consumers are sometimes required to pay upfront for medical care, or sometimes are refused access to care.<sup>36</sup>

To address this problem, we urge the Committee to amend the FCRA to obscure the names of creditors or collections agencies that may indicate the consumer's medical condition. We further recommend that the Committee shorten the obsolescence periods for negative information when

---

<sup>30</sup> 15 U.S.C. § 1681a(i).

<sup>31</sup> *Credit Score Accuracy and Implications for Consumers*, National Credit Reporting Association (NCRA) and the Consumer Federation of America (CFA), Dec. 2002, at <http://www.ncrainc.org/documents/CFA%20NCRA%20Credit%20Score%20Report.pdf>; Robert B. Avery, Paul S. Calem, & Glenn B. Canner, *An Overview of Consumer Data and Credit Reporting*, Federal Reserve Bulletin, Feb. 2003, at <http://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf>.

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

<sup>34</sup> *The Consequences of Medical Debt: Evidence From Three Communities*, Access Project, Feb. 2003, at [http://www.accessproject.org/downloads/med\\_consequences.pdf](http://www.accessproject.org/downloads/med_consequences.pdf).

<sup>35</sup> Jay MacDonald, *Medical Bills Can Make Your Credit Sick*, Bankrate.com, Aug. 28, 2002; Eve Tahmincioglu, *Is Your Health Insurance Hurting Your Credit*, New York Times, May 12, 2002.

<sup>36</sup> *Id.*; see also Hugh F. Daly III, Leslie M. Oblak, Robert W. Seifert, & Kimberly Shellenberger, *Symposium: Barriers to Access to Health Care*, Case Western Reserve Univ. Health Matrix: J. of L.-Med. (Winter 2002).



the collection and debt is insubstantial. Medical collections under \$250 should not stay on a report for seven years; a shorter time is more appropriate.

### **Congress should preserve the application of the FCRA to the background screening process**

A simple conviction or arrest for a minor crime can result in someone not being able to obtain a job—even one that requires minimal responsibility or does not involve security sensitivity. For example, Eli Lilly, in response to the September 11, 2001 attacks, hired ChoicePoint to perform investigations on thousands of contract workers.<sup>37</sup> Lilly's concern was reasonable enough—the company is the dominant producer of insulin in the world. But the result of the background checks was not reasonable. A pipe insulator at the company was fired for accidentally bouncing a \$60 check. One person was dismissed because the records check revealed a fourteen-year-old misdemeanor marijuana possession charge. Another was dismissed for a crime that he did not commit.

The FCRA addresses background checks by requiring employee consent, and by limiting the scope of the file for certain employees. A limited file (one that does not contain bankruptcies more than ten years old, other negative information more than seven years old, an other adverse information more than seven years old) is delivered to employers where the position pays less than \$75,000/year. This figure is too low in today's dollars.

Congress should limit the contexts in which a report can be obtained for employment purposes. These should be limited to jobs where employees handle large sums of money, or are genuinely security-sensitive. It is clear now that the current standard—consent—is too low, as even menial jobs require background checks.

The Committee should also close the loophole that allows employers to conduct their own employment screenings. Because of the availability of "no-questions-asked" background check companies on the Internet, there is heightened risk that employees could be unfairly harmed by the background check process. Employers must be required to obtain consent and disclose the results of background checks that they perform themselves and provide the source of the information to the individuals who are investigated.

Title VI of H.R. 2622 should be stricken and replaced with language that will improve accountability and accuracy in the background check process. Congress should not further limit or exempt background investigations from the FCRA. In large part, the FCRA was passed to address abuses of the investigative industry. If Congress chooses to remove the FCRA's important accountability provisions, it will lead to employees being fired or never receiving deserved opportunities because of errors or unfair practices.

---

<sup>37</sup> Ann Davis, *Firms Dig Deep Into Workers' Past Amid Post-Sept. 11 Security Anxiety*, Wall Street Journal, Mar. 12, 2002.



UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

Chris Hoofnagle, Deputy Counsel  
Epic.Org  
1718 Connecticut Ave. N.W.  
Suite 200  
Washington DC 20009

JUN 23 2003

Re: FOIA Request No. 2003-470  
Credit Bureau Complaints

Dear Mr. Hoofnagle:

This responds to your May 30, 2003, letter requesting access under the Freedom of Information ("FOIA") to the number of consumer complaints received by the Federal Trade Commission since January 1, 1997, pertaining to the credit bureaus Experian, Trans Union, and Equifax. Pursuant to the FOIA and agency policy, we have searched our records as of June 3, 2003, the date we received your request in our FOIA office.

A search of the Commission's records located two responsive pages and copies are enclosed. If you have any questions about the way we handled your request, or about our FOIA regulations or procedures, please contact Kathy Kelliher-Sloan (202) 326-3253.

Sincerely,

A handwritten signature in cursive script, appearing to read "Joan E. Fina".  
Joan E. Fina  
Attorney

Enclosure

Table 2. Complaints Against Equifax, Experian, or TransUnion by Calendar Year

Calendar Year 1997			
Credit Bureau	Non-Identity Theft	Identity Theft <sup>1</sup>	Total
Equifax	332	---	332
Experian	305	---	305
TransUnion	238	---	238

Calendar Year 1998			
Credit Bureau	Non-Identity Theft	Identity Theft <sup>1</sup>	Total
Equifax	1,923	---	1,923
Experian	1,964	---	1,964
TransUnion	1,799	---	1,799

Calendar Year 1999			
Credit Bureau	Non-Identity Theft	Identity Theft	Total
Equifax	2,285	23	2,308
Experian	2,860	26	2,886
TransUnion	2,374	12	2,386

Calendar Year 2000			
Credit Bureau	Non-Identity Theft	Identity Theft	Total
Equifax	2,744	282	3,026
Experian	2,629	275	2,904
TransUnion	2,263	146	2,409

Calendar Year 2001			
Credit Bureau	Non-Identity Theft	Identity Theft	Total
Equifax	3,932	495	4,427
Experian	2,957	365	3,322
TransUnion	2,726	143	2,869

Calendar Year 2002			
Credit Bureau	Non-Identity Theft	Identity Theft	Total
Equifax	5,291	2,681	7,972
Experian	4,221	1,800	6,021
TransUnion	3,494	504	3,998

Calendar Year 2003 <sup>2</sup>			
Credit Bureau	Non-Identity Theft	Identity Theft	Total
Equifax	2,094	896	2,990
Experian	1,882	672	2,554
TransUnion	1,756	236	1,992

<sup>1</sup>The FTC began accepting consumer inquiries and complaints about identity theft in October 1999.

<sup>2</sup>Calendar Year 2003 includes January 1 - June 3, 2003.

## FOIA 2003-470 Credit Bureau Complaints

Table 1. Complaints Against Equifax, Experian, or TransUnion by Calendar Year

Calendar Year	Non-Identity Theft	Identity Theft <sup>1</sup>	Total
1997	875	---	875
1998	5,633	---	5,633
1999	6,746	42	6,788
2000	6,253	478	6,731
2001	7,590	741	8,331
2002	11,158	3,399	14,557
2003 <sup>2</sup>	5,211	1,188	6,399

<sup>1</sup>The FTC began accepting consumer inquiries and complaints about identity theft in October 1999.

<sup>2</sup>Calendar Year 2003 includes January 1 - June 3, 2003.