



ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Electronic Privacy Information Center, Executive Director
Georgetown University Law Center, Adjunct Professor

With

Chris Hoofnagle, EPIC Deputy Counsel
Anna Slomovic, EPIC Senior Fellow

Hearing on
The Role of FCRA in Employee Background Checks
and the Collection of Medical Information

Before the

Subcommittee on Financial Institutions and Consumer Credit,
Committee on Financial Services,
United States House of Representatives

June 17, 2003
2138 Rayburn House Office Building

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today regarding the role of the Fair Credit Reporting Act (FCRA) in employee background checks and the collection of medical information. My name is Marc Rotenberg and I am the executive director of the Electronic Privacy Information Center (EPIC), a public interest research organization in Washington. I have taught Information Privacy Law at Georgetown University Law Center since 1990 and I am the coauthor, with Professor Daniel J. Solove, of *Information Privacy Law* (Aspen 2003). I have a long-standing interest in medical record privacy. I served on the Model State Public Health Privacy Law Project, directed by Professor Lawrence Gostin, and I wrote about the issue of preemption in the medical privacy field for the *Journal of Health, Law and Public Policy* in 1995.¹

Joining me this morning are Chris Hoofnagle and Anna Slomovic. Mr. Hoofnagle is Deputy Council of EPIC and concentrates on the Fair Credit Reporting Act. Ms. Slomovic, Ph.D., is the former Privacy Officer for a managed care organization.

This morning I will provide an overview of the ongoing problem of privacy protection, the scope of the medical privacy rule, and the need to protect medical information contained in credit reports. This issue should be of particular concern to this Committee because employers are increasingly using background checks on potential and current employees. Landlords are using credit reports to screen potential renters. Even health clubs use credit reports to evaluate applications for membership.

The widespread use of credit reports makes it more important than ever to ensure that medical information is not released inappropriately without the knowledge and consent of the individuals and without the necessary obligations that companies that collect and use personal information take on. Current federal and state laws protect medical information in many contexts. However, the protections are not always sufficient. I would like to discuss some of the ways in which medical information has been misused in the past, ways in which federal protection of medical information varies under different regulatory regimes, and states actions on protecting health information.

I. SCOPE OF PROBLEM

Protecting the privacy of medical information continues to be a serious problem in the United States. The misuse of an individual's medical data can result in real harms to that person. Privacy of medical information is undermined when an individual's medical records are not properly safeguarded, misused, or produce adverse and unfair outcomes.

One of the places where medical privacy invasion is felt most acutely is in the workplace. Opening up medical records to employers puts individuals at risk of discrimination based upon their medical conditions. Employees may be harassed, denied

¹ Marc Rotenberg, *Review: Institute of Medicine. Health Data in the Information Age: Use, Disclosure, and Privacy*. Washington, DC: National Academy Press, *Journal of Health, Law, and Public Policy* (Spring 1995).

medical insurance, fired, or subjected to any number of other negative consequences when their health records are disclosed to employers.

Today doctors are taking extraordinary measures to safeguard patients' files. Some doctors are withholding medical information from health records to help patients keep their medical history private. A recent survey of 344 members of the Association of American Physicians and Surgeons revealed that 87 percent of members surveyed reported that their patients had requested that they exclude data from patients' medical records, and 78 percent of those surveyed complied. In addition, almost one-fifth admitted to making false entries on medical records.²

The absence of effective medical privacy protection adversely affects the delivery of medical care. Janlori Goldman, Director of the Health Privacy Project at Georgetown University, observed in a recent survey for the California HealthCare Foundation revealed that one out of six people "withdraws from full participation in their own health care" because of fear that health care information will be used without their permission.³ The Labor, Justice, and Health and Human Services Departments found that 63% of individuals surveyed for a report would decline genetic testing if employers or insurers could obtain the results.⁴

Still another way an individual's medical information is misused and even exploited is when personal medical records are shared or sold for marketing purposes. Marketing provisions in medical privacy law permit "doctors, HMOs, and other healthcare groups to use personal patient data . . . for marketing purposes."⁵ Many on-line health sites collect information about visitors' browsing, buying and clicking habits. According to Ms. Goldman, "The business model of many health sites is based on the collection, use, and resell of personal health data." Many drug companies probably already know much more about us than we want them to.

The challenges of medical record privacy are likely to increase. Some companies are not only collecting medical information, but also DNA sample. Genelex, a genetics company in Redmond, Washington, "has amassed 50,000 DNA samples, many gathered surreptitiously for paternity testing." According to "CEO Howard Coleman[,] 'Siblings have sent in mom's discarded Kleenex and wax from her hearing aid to resolve the family rumors.'" However, whether or not the DNA is collected with an individual's knowledge, the data may be "stored without donors' knowledge. Cells banked for one purpose, such

² Dana Hawkins, *Guarding medical secrets, at a cost*, U.S. News & World Report, August 13, 2001.

³ Janlori Goldman and Zoe Hudson, "Virtually Exposed: Privacy And E-Health," *Health Affairs* (California HealthCare Foundation, Nov./Dec. 2000).

⁴ Joanne L. Hustead, Aimee Cunningham, & Janlori Goldman, *Genetics and Privacy: A Patchwork of Protections*, prepared for California HealthCare Foundation, Apr. 2002.

⁵ Dana Hawkins, *Medical privacy rules give patients and marketers access to health data*, U.S. News & World Report, Jan. 29, 2001.

as medical diagnosis, have been shared with or sold to other users for research or profit.”
6

II. LIMITATIONS ON CURRENT PROTECTIONS UNDER FEDERAL LAW

The HIPAA Privacy Rule is designed to protect health information by giving individuals greater control over this information and by limiting uses and disclosures that can be made without explicit individual authorization. Unfortunately, there appear to be several areas in which intended protections fail as health information moves from entities that must comply with the Privacy Rule to ones that are not required to do so. I will now describe the gaps between the HIPAA Privacy Rule and requirements under FCRA.

Definition of protected information is different in financial and health regulations

Under the Privacy Rule, protected health information (PHI) is broadly defined. Individually identifiable information is protected when it relates to an individual’s past, present, or future physical or mental health; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. The HIPAA definition of PHI includes information collected from an individual, as well as information created or received by a health care provider, health plan, employer, or health care clearinghouse.⁷

However, under FCRA, the term “medical information” is defined more narrowly. “Medical information” means information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics, or other medical or medically related facilities.⁸

This definitional difference means that some information protected under HIPAA does not receive protection under FCRA simply because it is not obtained from one of the entities listed in the FCRA definition.

Limitation on the types of entities covered by the Privacy Rule

Congress limited the regulatory authority of the Department of Health and Human Services (HHS) to three specific types of entities, called “covered entities”:

- Health care providers, who electronically transmit health information in connection with standard transactions
- Health plans
- Health care clearinghouses⁹

⁶ Dana Hawkins, *Keeping secrets: As DNA banks Quietly Multiply, Who is Guarding the Safe?*, U.S. News World Report, Dec. 2, 2002.

⁷ 45 CFR, §160.102 and §164.501.

⁸ 15 USC §1681a(1).

⁹ P.L. 104-191, SEC. 1172. (a) (“Applicability”).

Other entities may be subject to the Privacy Rule indirectly through business associate agreements if they are performing tasks “on behalf” of “covered entities.” Examples of business associates include billing companies, law firms, accounting firms, and third-party administrators. Business associate agreements must be in place before PHI is released to these entities. These business associate agreements must stipulate that a business associate will not use or disclose PHI for any purposes not specified in the agreement. The basic principle is that business associates acting on behalf of “covered entities” are subject to the same rules as the “covered entities” themselves with respect to the activities they perform under business associate agreements.

However, if an entity collects health information in a capacity other than “covered entity” or a business associate of a “covered entity,” it is not subject to the Privacy Rule. The Department of Health and Human Services acknowledges in the preamble to the December 2000 Privacy Rule that health information collected and used by life insurers, casualty/property insurers, auto insurers, worker’s compensation programs, employers and others is not subject to the protections of the Privacy Rule because these entities are outside the HHS statutory authority. It is, therefore, important that adequate protections for health information be provided in laws or regulations that govern these types of entities.

Limitation on protections of health information received by employers

HHS attempted to limit the use of health information by employers because such use could be particularly detrimental to individuals. In order to receive PHI from a “covered entity” employers generally need an individual’s signed authorization, explicitly stating by whom and for what purpose PHI is being obtained. In cases where an employer sponsors a group health plan, as defined under ERISA, the group health plan is not permitted to disclose protected health information to the employer plan sponsor without individual authorization until the plan receives a certification that plan documents have been amended to state that the sponsor agrees not to further use or disclose PHI except as permitted or required by law, and not to use health information for employment-related decisions.¹⁰

However, employers may receive health information from sources other than a “covered entity.” Health information received from such other sources is not protected under the Privacy Rule. HHS stated in its preamble to the December 2000 Privacy Rule:

With regard to employers, we do not have statutory authority to regulate them. Therefore, it is beyond the scope of this regulation to prohibit employers from requesting or obtaining protected health information. Covered entities may disclose protected health information about individuals who are members of an employer's workforce with an authorization. Nothing in the privacy regulation prohibits employers from obtaining that authorization as a condition of employment. We note,

¹⁰ 45 CFR, Part 164—Security and Privacy, 164.504, Uses and Disclosures, Organizational Requirements, (f)(1) Standard: Requirements for group health plans.

however, that employers must comply with other laws that govern them, such as nondiscrimination laws.¹¹

If an employer receives health information from a credit reporting agency or another source in the course of a background check on a current or prospective employee, the employer can use this health information in ways that are inconsistent with the Privacy Rule's intention to protect PHI from use or disclosure in employment-related actions without individual authorization.

Limitation on protection resulting from permitted activities

Another limitation on the protection of PHI that is of particular relevance here exists because the Privacy Rule disclosures to credit reporting agencies are part of payment-related activities of "covered entities." In order to facilitate the smooth operation of the health care system and the delivery of high-quality health care, activities related to treatment, payment and health care operations of "covered entities" do not require individual authorization. Disclosures related to these types of activities are also not subject to Accounting of Disclosures, which individuals can request from "covered entities" in order to learn what disclosures have been made without authorization.¹²

The PHI that may be disclosed to credit reporting agencies under the Privacy Rule is limited. The definition of "Payment" includes the following:

- (vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
 - (A) Name and address;
 - (B) Date of birth;
 - (C) Social security number;
 - (D) Payment history;
 - (E) Account number; and
 - (F) Name and address of the health care provider and/or health plan.¹³

Although limited, such PHI can, under some circumstances, lead the recipient to infer what medical services have been provided to an individual. Additional information can be gained by learning the specialties of providers who made the report.

As stated in the preamble to the December 2000 Privacy Rule, credit reporting agencies are not subject to the Privacy Rule unless they happen to be "covered entities." After the consumer reporting agency receives PHI, the information is subject to whatever

¹¹ 45 CFR, Parts 160 and 164—Security and Privacy, Preamble, Section III, Section-by-Section Discussion of Comments, Relationship to Other Federal Laws.

¹² 45 CFR, Part 164, § 164.528 (a)(1)(i).

¹³ 45 CFR, Part 164, § 164.501.

protections are afforded to such information under the regulations governing credit reporting agencies.¹⁴

Alternative Approaches to Protecting Medical Information Indicate Important Role of States

Entities that operate in multiple states look for a uniform regulatory environment in order to operate efficiently. For health insurers this includes the ability to consolidate service centers and other support operations in order to take advantage of efficiencies of scale and scope. As important as it is to improve efficiency of the health care system, however, federal preemption of state law is not the only way to obtain operational uniformity. State adoption of model laws and regulations is another way to create a uniform operating environment for organizations that operate in multiple states while providing states with the necessary flexibility to customize requirements for the needs of their citizens.

The National Association of State Insurance Commissioners (NAIC) has promulgated the Privacy Model Act that requires “opt-in” for sensitive health information, which is broadly defined. The NAIC Model Regulations, promulgated after the passage of Gramm-Leach-Bliley Act, closely track the requirements of that law for financial information, but provide more stringent protections for the more sensitive health information.

According to the NAIC, most states and the District of Columbia are adopting NAIC’s models.

- Twenty-four states planned to promulgate the NAIC Privacy of Consumer Financial and Health Information Model Regulation (the "NAIC model regulation") in its entirety, including the financial and health provisions.
- Nine states planned to promulgate only the financial privacy provisions of the NAIC model regulation. Several of these states already had health information protections in place or intended to follow up with health information protections in the future.
- Four states that previously adopted the 1982 NAIC Privacy Model Act planned to revise their current laws and/or regulations to be consistent with the NAIC model regulation’s notice and opt-out provisions for financial information; however, these states planned to keep the 1982 privacy model act’s opt-in requirement for health information privacy. The health privacy protections in the new model regulation also require opt-in before the disclosure of health information.
- Nine states planned to keep the 1982 model act in place.¹⁵

III. RECOMMENDATIONS

¹⁴ 45 CFR, Parts 160 and 164—Security and Privacy, Preamble, Section III, Section-by-Section Discussion of Comments, Relationship to Other Federal Laws.

¹⁵ NAIC press release, April 9, 2001.

1) Require that Medical Information Inferred from Credit Reports be Subject to Strong Protections

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.¹⁶

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.¹⁷ 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.¹⁸ Most of these collection items, however, are for small amounts. Sixty-six percent of medical collections are for amounts under \$250.¹⁹

Second, medical organizations are beginning to use more aggressive collections techniques.²⁰ Mounting evidence suggests that health care providers are more vigorously pursuing consumers because insurance companies frequently reject or dispute claims.²¹ 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

¹⁶ 15 U.S.C. § 1681a(i).

¹⁷ *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>.

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *The Consequences of Medical Debt: Evidence From Three Communities*, Access Project, Feb. 2003, at http://www.accessproject.org/downloads/med_consequences.pdf.

²¹ 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.

sometimes required to pay upfront for medical care, or sometimes are refused access to care.²²

To address this problem, we urge Congress 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 Congress shorten the obsolescence periods for negative information when 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.

2) Allow the Preemption Loophole to Expire

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.

Congress should not extend the preemption loophole into the future. 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 government, preemption should only be used in limited situations, and generally, preemption is not appropriate for consumer protection legislation.

Our current credit reporting system has thrived under a federal baseline of protections that is supplemented by dozens of stronger state credit reporting laws. We do not operate in a credit reporting system with a single, uniform standard. The Federal FCRA itself grandfathered in several state laws, including California, Vermont, and Massachusetts, as well as settlements made between the attorneys general and the credit reporting agencies.²³ Additionally, the states have passed laws regulating the content and costs of reports, and the duties of users and furnishers. States have passed many stronger privacy laws in many sectors.²⁴

Congress should not extend preemption in the FCRA because it will tie the hands of state legislators, and prevent them from performing in their traditional roles as “laboratories of democracy.” Justice Brandeis once noted that, “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.”²⁵

²² *Id.* at Fn. 9, *supra*; 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).

²³ 15 U.S.C. § 1681t.

²⁴ See Appendix. 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.

²⁵ *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (Brandeis, J., dissenting).

State laws have not, and will not balkanize the credit system. Under the Supremacy Clause, state legislation that conflicts with, frustrates, or prevents compliance with federal credit reporting laws is automatically preempted.²⁶

America's prior experience with privacy legislation clearly favors federal laws that allow states to develop complementary protections. 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.²⁷

Related areas of law allow states to formulate stronger protections. In areas such as freedom of information, civil rights law, and environmental regulation, states generally have the power to craft protections for their residents. Consumer protection, in general, is a state activity. Congress, despite giving the Federal Trade Commission (FTC) a consumer protection role, encourages states to create "mini-FTCs." As a result, all 50 states have consumer protection law on deceptive practices.

State legislators are rational actors that have accommodated the interests of consumers and businesses well. 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 fifty 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.

The report concludes: "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."

State consumer protection laws are more consumer friendly. State laws are more accessible to consumer litigants, and often offer longer statutes of limitations. State laws typically afford individuals private rights of action rather than remedies that require the action of a federal agency. They also enable aggressive attorney general action. State legislatures are better suited to tailor laws to communities. State legislatures are closer to their constituents, and are more likely to tailor a law to particular problems.

²⁶ *Hines v. Davidowitz*, 312 US 52 (1941).

²⁷ Respectively at 18 U.S.C. § 2510 et. seq., 12 U.S.C § 3401, 47 USC § 551, 18 USC § 2710, 29 USC § 2009, 47 USC § 227, 18 U.S.C. § 2721, and 15 U.S.C. § 6801.

Furthermore, information, more than any other product, can be tailored with technology in order to comply with disparate 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. If technology has given these companies the ability to discriminate among individuals who live on the same block; it can also enable these companies to comply with differing state requirements on credit.

3) Adopt Opt-In Framework for Affiliate Sharing

The problems described above will be exacerbated under the current affiliate-sharing rules that make it too easy for personal information concerning consumers, including transactions that reveal medical services and condition, to be disclosed to others and to be incorporated into consumer profiles.

We recommend that Congress adopt an opt-in framework to grant individuals greater control of their to medical, financial, and other information that may be shared among corporate affiliates. The complex corporate ownerships made possible by Gramm-Leach-Bliley pose new risks to individuals' privacy. Financial holdings companies may now amass a vast amount of information about their customers. Affiliates may include banks, insurance companies, securities firms, as well as institutions that significantly engage in financial activities, such as retailers that issue credit cards, auto dealerships that lease vehicles, and entities that appraise real estate. The law allows these companies to merge into large financial holding companies, and also merge their customers' data into one consolidated database. This data may include financial, medical and other sensitive information.

Some financial holding companies have thousands of affiliates, making it exceedingly difficult for consumers to understand what companies may have access to their sensitive information. CitiGroup, Inc., for example, has over 2,700 corporate affiliates.²⁸ Similarly, Bank of America has almost 1500.²⁹ Given this vast scope of possible affiliate sharing, we believe that opt-in is the best approach to apportion rights between individuals and business interests in affiliate sharing.

Having mentioned the scope of CitiGroup's affiliate network, it is important to note that Travelers Group, in its 1998 acquisition of Citicorp properties, agreed to keep its customer health and medical information confidential.³⁰ Travelers indicated that it would share medical information "only with the customer's consent or under very limited circumstances."³¹ This agreement demonstrates that even large, complex financial services entities can accommodate opt-in.

²⁸ *Financial Privacy and Consumer Protection Hearing Before the Senate Comm. on Banking, Housing and Urban Affairs*, 107th Cong., Sept. 19, 2002 (statement of William H. Sorrell, Attorney General, State of Vermont).

²⁹ *Id.*

³⁰ Federal Reserve Press Release (Sept. 23, 1998), at <http://www.federalreserve.gov/boarddocs/press/BHC/1998/19980923/19980923.pdf>.

³¹ *Id.* at 84.

IV. ADDITIONAL ISSUES

Mr. Chairman, I would like to bring to the Committee's attention two additional issues that are not specifically related to medical record privacy, but that do implicate the work of the Committee as it considers the ongoing importance of the financial privacy laws. The first issue concerns the expanded use of background checks. The second relates to information obtained just this week by EPIC, under the Freedom of Information Act, concerning the compliance with the privacy provisions contained in the Financial Services Modernization Act.

Employee background checks are being used more frequently as a result of the September 11, 2001 attacks.

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.³² 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 other provision that limits the content of the report if the job pays less than \$75,000, is also inadequate.

FTC Documents Obtained by EPIC under FOIA Indicate Ongoing Problems with Opt-out

Documents obtained this week by EPIC from the Federal Trade Commission, under the Freedom of Information Act, show that a majority of the complaints, received by the Commission, concerning compliance by large New York-area banks, with laws

³² Ann Davis, *Firms Dig Deep Into Workers' Past Amid Post-Sept. 11 Security Anxiety*, Wall Street Journal, Mar. 12, 2002.

that allow individuals to opt-out, are about Citibank. In fact, fifteen of the twenty total complaints were about alleged Gramm-Leach-Bliley privacy violations by Citibank.

Of those fifteen complaints, nine concerned failed attempts to opt-out. In one complaint, a consumer was told that he was already taken off the list, but continued to receive unsolicited credit card offers. In another complaint, a consumer reported that “Citibank will not allow her to opt-out.” Many of the complaints claimed that Citibank provided no phone number to opt-out with their unsolicited credit-card offers, and one complaint claimed that despite the fact Citibank provided online services, it did not have an online form to opt-out. Finally, in a complaint by a husband and wife, each was told to write a letter requesting to be removed from Citibank’s credit card offer list. Nevertheless, despite their letters, they continued to receive the unsolicited offers three months later.

These examples underscore the need for an opt-in. From this small sample, we can see that even where consumers take the time to write, call, or e-mail in order to opt-out, Citibank and other financial institutions fail to allow consumers to opt-out. Opt-out is simply not an effective means to safeguard consumer privacy. Opt-in is clearly preferable as the documents obtained from the FTC this week indicate.

V. CONCLUSION

Congress clearly intended to safeguard personal information through passage of the Fair Credit Reporting Act the legislation that led to adoption of the Health Insurance Portability and Accountability Act. But it is also clear that medical record privacy remains a critical concern in the United States today. EPIC urges the Committee to ensure that strong safeguards are established. Specifically, we support efforts to strengthen accuracy and access for credit reports. We further recommend proposal to give consumer control over pre-screening and limit affiliate sharing absent a clear opt-in provision. Most significantly, we urge the Committee to allow the state preemption loophole to expire. Our Constitutional form of democracy, and the development of privacy law and consumer law during the latter part of the twentieth century, made clear that the states must have the freedom to protect the interests of consumers. As we enter the twenty-first century, it is clear that privacy protection is one of the great issues facing the nation and that the states have a central role to play.

ABOUT EPIC

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and to promote the Public Voice in decisions concerning the future of the Internet. More information is available online at www.epic.org.

APPENDIX

Examples of Privacy Safeguards in State Credit Reporting Laws

- 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.
 - 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).