1999

Privacy and Accuracy of Personal Information

L. Richard Fischer

Follow this and additional works at: http://scholarship.law.unc.edu/ncbi

Part of the Banking and Finance Law Commons

Recommended Citation

Available at: http://scholarship.law.unc.edu/ncbi/vol3/iss1/5

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Banking Institute by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
PRIVACY AND ACCURACY OF PERSONAL INFORMATION

L. RICHARD FISCHER†

I. INTRODUCTION

During the past decade, there has been a substantially increased focus in the United States on the availability, use, and disclosure of personal information. This focus is usually described by the media, and by policy makers in Washington, as an increased public concern for personal privacy.

However, privacy represents only one part of this heightened public concern. There also has been an increasing focus on the importance of accurate information and on the security of information systems. Consumers (and thus policy makers) increasingly recognize that advancing technological developments permit greater access to and use of information to make offers to, and eligibility decisions with respect to, consumers, often before those consumers even apply for a loan, insurance, or other product. Thus, the policy debate in the United States today, particularly at the federal level, is not just about privacy, it is also about the accuracy of personal information.

II. SOURCES OF PRIVACY RIGHTS

A. Federal Privacy Rights

There is no single source of privacy rights in the United States governing personal information in privately owned or operated computer data banks. Instead, there is an extensive "patchwork quilt" of federal and state laws governing personal privacy. The Fourth Amendment to the U.S. Constitution prohibits unreasonable searches and seizures. However, this Constitutional provision does not restrict the information practices of private companies; instead, it generally is

construed to restrict only intrusive government activities. Even then, it has been held inapplicable to government efforts to obtain records, such as bank records in *United States v. Miller*.1

Beginning in the 1970’s, developments such as the advancing technology with respect to electronic banking and the electronic delivery of other services caused federal policy makers to focus on the need for the enactment of federal privacy statutes. On several occasions, federal policy makers have considered the possible adoption of a comprehensive privacy statute applicable to both private and governmental information systems.

For example, the United States Privacy Protection Study Commission identified a series of basic privacy principles in its Congressionally mandated 1977 report, and raised the possibility of comprehensive privacy legislation. In fact, Congress did establish such a comprehensive legal scheme for federal government information systems (or data banks) in enacting the Privacy Act of 1974.2 Rather than adopting a comprehensive privacy statute governing personal information in private data banks, however, Congress has addressed privacy protection in the context of specific industries or specific activities.

The following are examples of existing federal privacy statutes:

The Fair Credit Reporting Act of 1970 (FCRA)3 governs the information practices of consumer reporting agencies, such as credit bureaus, and the use of consumer reports and the sharing of affiliate information within bank holding companies and other multicompany organizations.

The Right to Financial Privacy Act of 19784 was enacted as a direct response to the Miller decision, and established notice and access procedures for access to financial information by federal government agencies. The same is true of the corresponding tax law provisions governing access by the IRS to financial institution records.5

---

The Electronic Fund Transfer Act of 1978\(^6\) provides a basic framework establishing the rights, liabilities, and responsibilities of parties with respect to electronic fund transfers. Its primary objective is to protect the rights of individuals in such transfers. It also requires notice of the circumstances when account information will regularly be disclosed to third parties.

The Comprehensive Crime Control Act of 1984 made it a federal crime to access certain computer systems and obtain information without authorization.\(^7\) Congress elected to limit the focus to computer systems involving a compelling federal interest, such as computers maintained by the federal government or computers maintained by federally insured financial institutions.

The Cable Communications Policy Act of 1984,\(^8\) as amended by The Cable Television Consumer Protection and Competition Act of 1992, restricts the collection, use and disclosure of information relating to cable systems.

The Electronic Communications Privacy Act of 1986\(^9\) is intended to protect against unauthorized interception of electronic communications.

The Computer Fraud and Abuse Act of 1986\(^10\) made it a federal crime to "knowingly" access certain computer systems and obtain information without authorization. The intent of Congress was to proscribe intentional acts of unauthorized access and focus federal criminal prosecutions on individuals whose conduct evidenced a clear intent to enter, without proper authorization, computer files or data belonging to a financial institution.

The Telephone Consumer Protection Act of 1991\(^11\) was created to govern telephone solicitations and give the Federal Communications Commission the rulemaking authority to prescribe regulations necessary to protect residential subscribers' privacy by avoiding telephone solicitations to which they object.

\(^10\) Id. § 1030.
The Identity Theft and Assumption Deterrence Act of 1998\textsuperscript{12} amended the federal criminal code to make it a crime for a person to knowingly transfer or use, without lawful authority, a means of identification of any other person with the intent to commit, aid or abet any unlawful activity that violates federal law.

\textbf{B. Federal Privacy Policy Develops Against the Backdrop of State Privacy Rights}

Several state constitutions contain express provisions protecting privacy rights. For example, the California Constitution contains a specific privacy provision. Other states have search and seizure provisions that, unlike the result in \textit{United States v. Miller},\textsuperscript{13} have been interpreted to protect individual privacy rights. Usually these constitutional privacy provisions are interpreted as creating reasonable expectations of privacy. Thus, in attempting to apply such privacy protections, one must consider whether the particular use or disclosure was, or should have been, within the reasonable expectation of the particular consumer or class of consumers.

Moreover, state common law privacy rights have developed as a result of decisions in several states regarding the disclosure of customer information, particularly the disclosure of account information by financial institutions. Most commonly these decisions involve the use of deposit account information by financial institutions and focus on the special relationship between financial institutions and their customers. Generally, these decisions focus on privacy as an implied contract right, but "implied contract" is simply another way to characterize "reasonable expectations."

State statutory provisions relating to personal privacy are becoming more common. Certain states, such as Massachusetts and Wisconsin, have adopted more general privacy statutes. Other states have adopted industry-specific statutes dealing with particular entities, including consumer-reporting agencies. For example, a New Jersey statute permits the disclosure of information relating to electronic fund


\textsuperscript{13} United States v. Miller, 425 U.S. 435 (1976); see also supra note 1 and accompanying text.
transfers only under certain circumstances, such as with consumer consent or where it is necessary to complete the transaction. 14 More recently, states have begun to restrict the disclosure of certain credit card information. 15 As is the case at the federal level, it is likely that state legislatures and courts will continue to focus on privacy-related issues.

C. Industry Privacy Principles as a Source of Individual Privacy Rights

For many years, individual financial institutions and companies, and their associations, have adopted and disclosed privacy policies or statements of information practices. In many instances, these policies are provided to customers separately. In others, they are incorporated into customer contracts, account agreements or customer rules. In some cases for financial institutions, the description of information practices is accomplished through an amendment to the disclosure required by Regulation E for accounts that are accessible by electronic fund transfers. 16

In 1997, the American Bankers Association, the Consumer Bankers Association, The Bankers Roundtable, and the Independent Bankers Association of America announced joint industry privacy principles and recommended their adoption by members. Other groups of companies, particularly on-line service providers, have established similar industry privacy principles. Although the adoption of such privacy policies or privacy principles may be done in the first instance on a voluntary basis, it is important to recognize that the incorporation of such principles into customer agreements, or even the communication of such principles to individual customers, can create enforceable rights for customers. First, as noted above, the basis of common law privacy rights is the reasonable expectations of customers, and the adoption and publication of privacy principles by a financial institution or other company clearly can shape those expectations.

In addition, existing federal law makes unlawful "unfair or deceptive acts or practices in or affecting commerce." \(^{17}\) Section 18(f)(1) of the Federal Trade Commission Act (FTC Act) prescribes unfair and deceptive practices by banks. \(^{18}\) Although Federal Reserve Regulation AA, promulgated under section 18(f)(1), by its terms focuses on unfair and deceptive credit practices, \(^{19}\) the underlying statute is much broader in scope. Moreover, for banks the enforcement mechanisms of the Federal Deposit Insurance Act \(^{20}\) also are applicable. \(^{21}\)

Therefore, the statement by a bank of its privacy policies or principles that does not accurately reflect the information practices of that bank can give rise to a cause of action under current state common law privacy principles. The publication by a bank or other company of privacy policies that are substantially inconsistent with the actual information practices of that bank or other company also can create exposure for unfair and deceptive practices under existing federal law.

A good example of this is the FTC's action against GeoCities because the FTC concluded that actual information practices of GeoCities were not consistent with the privacy policies it disclosed to its customers. \(^{22}\) In addition, most states have enacted mini-FTC Acts that may give rise to similar customer rights under existing state law.

D. Influence of International Privacy Developments

In the mid-to-late 1970's, while the United States decided not to enact comprehensive privacy laws governing private information systems, the governments of certain other nations elected to adopt more far-reaching data protection laws. For example, the Organization for Economic Cooperation and Development (OECD) developed "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," which were adopted by the


Council of Ministers in 1980. The OECD included governmental representatives from Western Europe, New Zealand and Japan. More recently, other nations, such as Canada and Japan, have adopted updated laws intended to protect personal information contained in developing data systems.

In 1995, privacy efforts in Europe took a more comprehensive statutory approach with respect to private information systems when the Council of Ministers and the Parliament of the European Union (EU) adopted a directive on personal data privacy.\textsuperscript{23} By its terms, that Data Protection Directive applies to all processing of personal data by any person or organization whose activities are governed by EU law and, thus, provides comprehensive privacy standards for both private and governmental databases. The overall effective date of the Data Protection Directive was October 25, 1998 and each individual member nation is directed to adopt implementing legislation.

The Data Protection Directive establishes an obligation to collect data only for specified, explicit and legitimate purposes and to maintain that information only if it is relevant, accurate and up-to-date. The Data Protection Directive establishes a principle of fairness regarding the collection of data under which each individual is given the option of whether to provide the information requested or not, through a type of notice and opt-out procedure. Individuals also must be provided with an opportunity to learn the identity of organizations intending to process data about them and the main purposes for which that information is being collected, or will be used.

The Data Protection Directive also requires all data processing to have a proper legal basis and identifies the following legal grounds for the collection and use of data: (1) consent; (2) contract; (3) legal obligations; (4) vital interests of the data subject; and (5) the balance between the legitimate interest of the people collecting or using the data and the people to whom the data relates.

In addition, the Data Protection Directive provides data subjects with a number of rights, including: (1) the right of access to data; (2) the right to know where the data originated; (3) the right to have inaccurate data rectified; (4) the right of recourse in the event of

unlawful processing of data; and (5) the right to withhold permission
to use their data in certain circumstances.

Importantly, where data is transferred from an EU country to a
non-EU country, the Data Protection Directive establishes a basic rule
that the non-EU country receiving the data must provide an "adequate
level" of data protection.\textsuperscript{24} It is important to note that Article 25 uses
the phrase "adequate level," not "comparable level" or "similar
level."

Under Article 25, an inquiry about a potential receiving
country's privacy standards can be raised by the transmitting country,
by another EU-member nation, or by the EU staff in Brussels. Article
25(2) provides that an adequate level of privacy protection is assessed
in light of all circumstances surrounding the data transfer operation,
including: (1) the nature of the data; (2) the purpose and duration of
the data processing and transmission operation; (3) the rules of law in
force; and (4) the professional rules and security measures established
for the data.

Article 26 identifies the circumstances under which an EU-
member nation can authorize transfer in the absence of an adequate
level of data protection, including: (1) the data subject has given
consent to the transfer unambiguously (it is not clear whether
affirmative assent is required, or if notice and opt out is sufficient);
and (2) the company receiving the data establishes privacy rights
through appropriate contractual clauses. Thus, the Data Protection
Directive could preclude the transmission of personal data outside the
EU to countries that lack an "adequate level" of privacy protections.

High-level representatives of the Clinton Administration and
the EU Commission have been working to avert a potential "trade
war" over electronic commerce and other problems that might arise
because of the implementation of the Data Protection Directive. There
have been indications that these meetings have had a positive effect,
but success is still far from certain. Although the U.S. and European
Commission failed to agree on data privacy in a meeting held in
Brussels on October 15, 1998, the EU-member states on October 26,
1998 endorsed the Commission's efforts to reach a negotiated
understanding on data privacy with the U.S. Although the parties

\textsuperscript{24} See \textit{id.} at art. 25.
were unable to reach agreement by year-end 1998, efforts are continuing.

By endorsement of such negotiations, EU-member states also hoped to avoid disruption of data flows to the U.S. while the negotiations are taking place. Individual access to data remains one of the major issues to be decided. The EU is insistent that individuals be allowed to access information on-line and also be able to correct inaccuracies in the information.

Undersecretary of Commerce Aaron has stated that one possible approach to take during the negotiations will be to attempt to provide a “safe harbor” for U.S. firms that follow certain privacy principles. On November 5, 1998, the Department of Commerce issued a draft safe harbor proposal (Draft Proposal). Under the Draft Proposal, a company would qualify for the safe harbor if it is subject to a statutory, regulatory, administrative or other body of law that effectively protects personal information privacy.

An entity also could qualify for the safe harbor through individual company or other private-sector-developed privacy programs that adhere to certain privacy principles (Principles) set forth in the Draft Proposal. The information accompanying the Draft Proposal emphasizes that the Principles are intended solely for the purposes of qualifying for the proposed safe harbor and are not intended to govern or affect internal U.S. privacy rules, which are being addressed by other government and private sector efforts.

Under these Principles an organization would be required to do six things. First, the organization must clearly and conspicuously inform individuals about the types of personal information it collects about them, how it collects that information, the purposes for which it collects such information, the types of organizations to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.

Second, the organization must give individuals the opportunity to choose whether and how personal information they provide is used where such use is “unrelated” to the use for which the information was originally disclosed (for certain types of “sensitive information such as medical information,” affirmative consent would be required).

Third, the organization must require that third parties to which personal information is transferred provide at least the same level of
privacy protection as originally chosen by the individual.

Fourth, the organization must keep only that personal data which is relevant for the purposes for which it has been gathered and take reasonable steps to ensure the reliability of data and to protect information from loss, misuse or unauthorized access.

Fifth, the organization must provide individuals with “reasonable access” to information about them and an opportunity to correct or change inaccurate information.

Finally, the organization must provide enforcement mechanisms to assure compliance with the Principles. The Draft Proposal states that organizations can satisfy the Principles’ enforcement requirements through compliance with “legal or regulatory supervisory authorities” or by committing to cooperate with data protection authorities in the EU.

The EU issue is important not only because of its implications for companies that do business internationally and for e-commerce, but also because it provides additional leverage to those who advocate that Congress should enact more restrictive privacy protections here in the United States.

III. EXPANSION OF PRIVACY RIGHTS

A. Prospects for Broader Federal Privacy Statutes

As originally proposed, the Privacy Act of 1974 would have been applicable to private information systems, as well as to government data banks.

The Privacy Commission suggested the adoption of more comprehensive privacy principles. In nearly every Congress, legislation is introduced to create a more comprehensive scheme for federal privacy protection, including the creation of a federal data protection board similar to that in many European countries. To date, however, Congress has not enacted comprehensive privacy legislation and it is unlikely to do so in the near future.
B. Increasing Federal Focus on Privacy Protection

The National Telecommunications and Information Administration (NTIA) advises the Secretary of Commerce and the President on domestic and international communications issues, and on related economic and technological advancement in the United States. In October of 1995, the NTIA released a report on privacy, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, which was prepared by a project team headed by Jerry Kang, Acting Professor, UCLA School of Law. The focus of the paper is privacy in the telecommunications sector, including telephone and video services.

On April 28, 1997, the Office of Management and Budget, on behalf of the Privacy Working Group, announced that it was seeking comments on Options for Promoting Privacy on the National Information Infrastructure (Options Paper). The Options Paper builds upon the Privacy Working Group’s Principles and sets forth several approaches to address privacy-related issues, including the possible creation of a federal privacy agency with full regulatory authority.

In January 1998, the NTIA and the Commerce Department jointly released a discussion draft of a report entitled *Elements of Effective Self-Regulation for Protection of Privacy* (Privacy Paper). On June 5, 1998, the agencies solicited comment on the Privacy Paper. The Privacy Paper attempts to identify elements of effective self-regulatory regimes, including principles of fair information practices and enforcement mechanisms that attempt to ensure compliance with those practices.

Not surprisingly, the Elements of the Privacy Paper are similar to the Principles in the Commerce Department’s “safe harbor” Draft Proposal. The Privacy Paper recommends that, at a minimum, consumers should be informed of the identity of the collectors of their personal information, the intended uses of that information, and the means by which consumers may limit its disclosure.


The Privacy Paper also suggests that companies that collect and use personally identifiable information should develop privacy policies that are distributed to consumers and which articulate the manner in which the company will collect, use, and protect data. In addition, the Privacy Paper states that consumers should be given the opportunity to exercise choice with respect to whether and how their personal information is used, either by businesses with whom they have direct contact or by third parties.

Moreover, the Privacy Paper states that companies that create, maintain, use, or disseminate records of identifiable personal information should take reasonable steps to assure its reliability for its intended use, and should take reasonable measures to protect such information from loss, misuse, alteration, or destruction. Furthermore, the Privacy Paper recommends that consumers be given an opportunity for access to information about them that is held by a company, and be able to correct or amend that information when necessary. The Privacy Paper also provides suggestions regarding enforcement mechanisms which attempt to ensure compliance with the principles for fair information practices described above, and which provide recourse for an individual when such practices are not followed. In addition, the Privacy Paper suggests that companies should take steps to verify that their privacy practices are effective and have been implemented as represented.

In another Clinton Administration initiative, the Commerce Department has conducted high profile conferences discussing the Privacy Paper as well as other privacy issues, such as the role of government in protecting privacy and whether federal privacy legislation is needed. The Commerce Department used these conferences to gather information for its report to President Clinton assessing the progress of industry self-regulatory efforts with respect to privacy protection on the Internet. On July 1, 1997, the Clinton Administration issued a report entitled *A Framework for Global Electronic Commerce* (Framework), which summarized the Administration’s views at that time regarding a number of privacy-related issues. In the Framework, the Clinton Administration indicates that it continues to support private sector efforts to implement meaningful, self-regulatory privacy regimes. The Framework also states that the Administration believes that these private efforts are
preferable to government regulation, but indicates that if private efforts fail to produce effective privacy protection, the Administration will reevaluate this policy.

In addition, the Framework notes that many countries around the world have enacted laws, implemented industry self-regulation, or instituted administrative solutions designed to safeguard their citizens' privacy. According to the Framework, the Administration will engage in discussions with key trading partners to build support for industry-developed solutions to privacy problems to ensure that differing privacy policies around the world do not impede the flow of data on the Internet. The Framework also states that the Clinton Administration will continue to engage in policy discussions with the EU nations and the European Commission, to increase their understanding of the U.S. self-regulatory approach to privacy.

On July 31, 1998, Vice President Gore called for the establishment of an "electronic bill of rights." The Vice President called for action to protect sensitive personal information, stop identity fraud, and encourage voluntary private sector action to protect privacy. He indicated that legislation in some areas might be necessary to accomplish these goals.

The FTC has been very active in the privacy arena as well, conducting a number of privacy workshops focused particularly on online privacy issues. It also has released a number of statements and reports on privacy-related issues. On June 4, 1998, the FTC released Privacy Online: A Report to Congress. The report revealed that only 14% of the commercial web sites surveyed provide any notice of their information collection practices. According to the report, approximately 2% provide a comprehensive privacy policy.

In connection with the report's release, FTC Chairman Pitofsky stated that "more incentives are necessary to encourage self-regulation and to ensure consumers that their personal information will be protected on line." Chairman Pitofsky also has stated that if efforts to encourage voluntary compliance are unsuccessful, legislation may be necessary.

Much of the recent regulatory activity in the privacy area has
originated from federal banking agencies. In April of 1998, the Consumer Electronic Payments Task Force established by the Department of Treasury released a report, which concluded, among other things, that consumer concern about use of personally identifiable information, if unaddressed, could act as an impediment to widespread acceptance of e-money and use of e-commerce.

On August 17, 1998, the Federal Deposit Insurance Corporation (FDIC) released *Online Privacy of Consumer Personal Information.* The FDIC supports industry self-regulation to address consumer privacy issues and encourages financial institutions to maintain an awareness of emerging technology privacy concerns. The FDIC indicates that institutions should take voluntary, specific actions to address those concerns and should provide meaningful disclosures of their privacy policies and information practices and effectively enforce them.

The Office of the Comptroller of the Currency (OCC) also has been active on the privacy front and has released several statements on the privacy efforts and obligations of national banks. On October 19, 1998, the OCC convened a Privacy Forum, at which representatives of the financial industry, consumer groups, and government staff discussed various privacy issues.

On November 3, 1998, the Office of Thrift Supervision issued its *Policy Statement on Privacy and Accuracy of Personal Customer Information* (Policy Statement). The Policy Statement explains that: (1) thrift institutions have an obligation to maintain and protect confidential and accurate customer information; (2) institutions should establish adequate controls to make sure that customer information is protected and used as agreed with the customer; and (3) institutions should notify customers and customers should be given the opportunity to limit or opt out of information use if institutions want to use customer information for purposes other than their own internal business purposes, such as for cross-marketing products of an affiliate.

On October 30, 1998, President Clinton signed into law H.R.

---


The legislation amends the federal criminal code to make it a crime for a person to knowingly transfer or use, without lawful authority, a means of identification of any other person with the intent to commit, aid or abet any unlawful activity that violates federal law or constitutes a felony under applicable state or local law. “Means of identification” includes any name or number that may be used to identify an individual. The legislation also directs the United States Sentencing Commission to review and amend the federal sentencing guidelines to provide for an appropriate penalty for these offenses. In addition, it directs the FTC within one year to establish procedures to receive identity fraud complaints, provide information to the victims and refer the complaints to appropriate entities.

C. New Federal Rules on Affiliate Sharing Have Broad Implications for All Companies

Historically, federal banking agency and FTC interpretations of the FCRA restricted affiliated companies from fully capitalizing on customer information sharing. In particular, agencies interpreted the FCRA to treat affiliated companies as if they were unrelated third parties. Banks and other companies often refrained from sharing customer information with members of their own corporate family. If a bank or other company shared non-experience information, such as application information, with one of its own affiliates, it risked being classified as a consumer reporting agency subject to all of the restrictions and requirements imposed by the FCRA on credit bureaus.

These agency interpretations and the resulting information sharing restrictions limited the ability of companies and their affiliates to identify potential customers and cross-market products and services. It also limited their ability to control risk by obtaining and considering problem credit information already in the possession of an affiliate.

The 1996 FCRA amendments clarify that affiliated companies may share, without limitation, so-called “experience information.” That is, an affiliate may share with another affiliate in the same

corporate family any information that consists of the transactions or experiences between one of the affiliates and the consumer to whom the information relates. This information can be shared either directly between the two affiliates or through a central database maintained by a designated member of the corporate family.

The amendments also allow affiliates to share, either directly or through a central database, any other information provided that it is clearly disclosed to the consumer that such information may be shared among the affiliates and the consumer is given an opportunity to opt out of the sharing before it takes place. For example, under the revised FCRA, members of the same corporate family may share among themselves (but not with unrelated third parties): (1) application information; (2) information from demographic firms; (3) credit reports from credit bureaus; and (4) any other information.

Privacy expectations are addressed through the notice and opt-out process. The notice and opt-out opportunity can be provided to new customers by, for example, adding appropriate language to application forms and account agreements.

Companies also should take appropriate internal measures to safeguard the security of customer information, as well as to develop internal policies on the use of customer information.

The amendments preempt completely any state law or regulation governing information sharing among affiliated companies. Thus, for example, the preemptive effect can extend beyond state fair credit reporting statutes to other state laws that purport to restrict information sharing among affiliated entities.

D. The FCRA and the Quality of Consumer Records

The FCRA is intended by Congress to have a positive impact on the quality of information regarding consumers. Historically, the FCRA has focused primarily on credit bureaus, rather than companies using credit bureau information. In fact, until the FCRA was amended in the fall of 1996, it imposed only limited requirements on companies using credit bureau information including: (1) permissible purpose

32. See id. § 1681a(d)(2)(A)(iii).
rules (including those for prescreening); (2) affiliate sharing limitations; and (3) adverse action notice obligations.

The quality of credit bureau files has been a major policy issue, both for Congress and state legislatures, for years. For example, the FTC indicated at one point that nearly 20% of all complaints it received related to credit bureau inaccuracies. The FTC staff believed that a significant percentage of these complaints resulted from split files or mixed files at credit bureaus. When challenged, the credit bureaus often say that the problem is caused by creditors and others who furnish information to credit bureaus. They say that it is a result of "garbage in, garbage out."

There are three principal complaints or criticisms that credit bureaus have directed at credit grantors: (1) the data provided is often inaccurate; (2) credit grantors and others often do not respond to reverification requests; and (3) even when they do respond, they often do not correct their own records and, thus, they report the same bad information again the following month. Congress believes that it addressed these "problems" or perceived problems when it amended the FCRA in 1996.

Many companies, including banks, supported the federal FCRA amendments. This is because there are several provisions of the FCRA legislation that banks supported, such as (1) prescreening clarification, including postscreening flexibility; (2) affiliate sharing; and (3) federal preemption.

The FCRA amendments also include several new requirements for creditors and others who furnish information to credit bureaus. For the first time accuracy requirements are established for companies that furnish information to credit bureaus. 33

For example, a company is prohibited from furnishing information to a credit bureau that a company knows (or consciously avoids knowing) is incomplete or inaccurate. The "knows" standard is subject to interpretation and therefore provides some uncertainty. It will cause most companies to specify an address that consumers can use to challenge information furnished to credit bureaus. It also will require companies to establish procedures to respond to consumer inquiries and to correct records at all bureaus to which they report

33. See id. § 1681s-2.
Companies now also have an affirmative duty to correct and update information they furnish to credit bureaus. The correction responsibility applies, for example, when a company is informed of an error by either the credit bureau or the consumer. It also applies if the company discovers the error itself. When a company discovers that it has incorrectly or incompletely reported information to one or more credit bureaus, it must report accurate or complete information to each credit bureau to which it had earlier provided inaccurate information.35

Companies have a duty to provide notice of a “continuing” dispute with the consumer when they continue to report disputed information to credit bureaus.36 This is similar to the existing requirement under federal and state fair credit billing laws. This provision contemplates that a company, for example, has first reinvestigated the dispute and determined that its records are correct. If the consumer then continues to dispute the accuracy of that information, the company cannot subsequently report that information to a credit bureau without also indicating that the consumer continues to dispute that information.

Creditors also are obligated to notify credit bureaus when a consumer voluntarily closes a credit account.37 This notice requirement does not apply when the account is closed because of delinquency or payment disputes. However, it applies when the consumer returns the card or otherwise instructs the creditor to close an account that is in good standing. Therefore, a creditor must have procedures in place to notify credit bureaus that the consumer has voluntarily closed an account, whether or not the consumer requests the creditor to provide such a notification. The creditor must report the voluntary account closing to each bureau to which it has been reporting information on that account.

Creditors are obligated to report the month and year of the start of a consumer’s delinquency that leads to a charge-off.38 This requirement is designed to enable credit bureaus to use that date to

34. See id. §§ 1681s-2(a)(2) and 1681s-2(b).
35. See id.
36. See id. § 1681s-2(a)(3).
37. See id. § 1681s-2(a)(4).
38. See id. § 1681s-2(a)(5).
start the seven-year time frame for reporting adverse information. At the end of that seven-year period, the information can no longer be included in most credit reports issued by a credit bureau. To satisfy this requirement, a creditor must be able to identify the commencement date of the credit problem that led to the charge-off. In most cases, the creditor should be able to do so by reporting a date consistent with that used for the application of its regulatory-mandated or accounting-based charge-off policy.

Finally, and perhaps most importantly, companies are obligated to respond to a notice from a credit bureau about a dispute regarding the accuracy of information reported by the company to the credit bureau. The time period to research the matter and respond to the dispute notice is very short—no more than thirty days.\(^{39}\) This time frame is the maximum permitted for completing everyone’s compliance efforts, including the credit bureau (and the credit bureau gets at least ten of those thirty days). This does not leave much compliance time for reporting companies. In addition, a reporting company is prohibited from resubmitting the old information to the credit bureau without first certifying the accuracy of that information. Thus, reporting companies must have procedures to ensure that their own records regarding that consumer have been corrected, as well as the records of the consumer at the credit bureau.

All of these requirements will be enforced by federal agencies. For banks, enforcement will be by federal banking agencies. For most others, enforcement will be by the FTC. In addition, state attorneys general are given authority to enforce compliance with these various “furnisher” obligations. These new obligations for companies that report information to credit bureaus, including the reinvestment requirements, will place a high premium on automated reporting and reinvestment procedures, and on coordinated efforts to get accurate information to all of the nationwide credit bureaus in a timely fashion.

\(^{39}\) See id. §§ 1681s-2(b)(1) and (2).