

Fair and Accurate Credit Transactions Act: More Protection for Consumers

Businesses must heed FACTA requirements for protecting consumers' credit records or face criminal or monetary consequences

Stacey Moyer

The Fair and Accurate Credit Transaction Act (FACTA) was signed into law on December 4, 2003, amending the capstone consumer credit statute, the Fair Credit Reporting Act (FCRA), which was enacted in 1970. Both laws are designed to provide consumers with the ability to safeguard their sensitive, personally identifiable financial information and to grant a federal entity – the Federal Trade Commission (FTC) – with enforcement tools when consumer data is used inappropriately.

In a sense, FACTA is the strong arm of a series of statutory regimes intended to protect consumers. FACTA aims to protect consumer financial information, such as credit reports or banking account information. Other federal regimes, such as the Health Insurance Portability and Accountability Act (HIPAA), govern the safekeeping of personally identifiable health information. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, also known as CAN-SPAM, applies to transmissions of unsolicited electronic mail into personal e-mail boxes. Other statutes aim to

protect trade secrets, national security, and Social Security numbers.

Identity Theft Continues to Grow

The FTC, the federal agency charged with enforcing consumer statutes, indicates in a recent report that more than 645,000 identity theft complaints were made to the agency in 2004. An FTC survey the previous year showed that identity theft had cost U.S. businesses nearly \$48 billion and consumers \$5 billion in losses. Restoring good credit is also time-consuming; identity theft victims had spent more than 300 million hours attempting to correct their credit records.

The problem of identity theft has come to the attention of lawmakers on Capitol Hill. Lawmakers have debated a

At the Core

This article

- ▶ Reviews the advent of consumer protection laws
- ▶ Highlights the role of the states in enforcing laws
- ▶ Describes the rights of consumers under the laws

FACTA: At a Glance

The Fair and Accurate Credit Transactions Act (FACTA) changed existing consumer credit law. Some of the new provisions enacted in FACTA include:

- Requiring fraud alert notices to be presented to the consumer in a manner that is clear and conspicuous
- Requiring a Consumer Reporting Agency (CRA), upon consumer good faith allegation and direct request, to include a fraud alert in the consumer's file for at least 90 days ("one-call fraud alert")
- Requiring the CRA to inform the consumer that the consumer may request a free copy of the consumer's file
- Requiring a CRA to notify other CRAs of the fraud alert
- Mandating truncation of credit card and debit card numbers, allowing the printing of no more than the last five digits

number of bills aiming to prevent the theft of sensitive personal information, but no single measure has emerged to be the primary legislative vehicle for an overarching federal identity theft bill. A number of states, weary of waiting for the federal government to act, have enacted tough laws designed to prevent identity theft and impose stringent penalties on lawbreakers.

FCRA Parameters

FCRA gives states authority of enforcement and does not preempt state credit reporting laws unless the state law is inconsistent with FCRA. State laws may not address information contained in a consumer report, the responsibilities of those furnishing information to consumer reporting agencies, actions that a consumer reporting agency (CRA) must take regarding the dispute of inaccurate information (unless the state law was in effect before September 30, 1996), or refer to any duties of any person who takes an adverse action against a consumer based on information contained in the consumer report. Likewise, the FTC may enforce state consumer laws.

A number of entities are affected by FCRA (See "FCRA Covered Entities," p. 64). A CRA is an entity that regularly assembles, evaluates, and maintains information for the purposes of reporting to third parties on an individual's credit worthiness. CRAs may use public records to gather information about an individual's credit standing (e.g., whether a person has declared bankruptcy, owes child support, or has a lien on any property they own).

FCRA defines a consumer report as "written, oral, or other communication of any information by a consumer reporting agency bearing on the consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living." Information is expected to be used to fashion a report "establishing the consumer's eligibility for credit or insurance, to be used for personal, family, or household purposes, employment, or any

authorization of extension of credit by issuer of credit card." The consumer report is required to include Title 11 bankruptcy filings, child support obligations, and credit scoring information.

Some information is strictly prohibited from being included in the consumer report. For example, consumer report information may not be used for employ-

ment purposes or credit or insurance transactions without written consumer consent. Information relating to transactions arising from the receipt of medical services, products, or devices and information sought by law enforcement agencies relevant to national security investigations are exempted.

Other prohibited information

FCRA Covered Entities

The Fair Credit Reporting Act, which the recently passed FACTA amends, applies to those who

- Compile and maintain data files on consumers, i.e., consumer reporting agencies
- Procure consumer reports for resale
- Furnish information included in consumer reports
- Use consumer reports – including employers who use credit reports in hiring decisions.

includes information from public records pertaining to tax liens, criminal records, outstanding judgments, and civil actions unless the accuracy of the information has been verified. Information about Title 11 bankruptcy filings that is more than 10 years old must be expunged from the consumer report. Arrest records and information on civil actions must also be expunged from the consumer record after seven years or until the statute of limitations on the particular action has expired (whichever is longer). Paid tax liens and accounts placed in collection or charged to profit or loss that are more than seven years old must also be removed. Any other adverse information, aside from records about a criminal conviction, must also be removed after seven years.

FCRA contains a general prohibition on including adverse information that is obtained via personal interview unless the CRA has cross-checked other verifiable sources to ensure the information is correct. CRAs are required to ensure that information in the report is correct and must protect the information against identity theft. Users of credit report information are required to verify their identity to the CRA, unless they are law enforcement agen-

cies seeking the report for investigations affecting national security.

Employers seeking access to consumer reports for employment purposes must have the consumer's written permission. For employment actions that will be reported to the CRA, the employer must provide notice to the consumer along with steps that he or she may take to dispute the information.

Consumer reports may be used in a wide variety of situations. (See sidebar below.) The information may also be used by national security agencies during investigations. Consumer report information must be provided to the Federal Bureau of Investigation if it pertains to national security matters or to any other governmental agency authorized to conduct investigations of international terrorism. Special rules allow CRAs to furnish basic information – such as consumer name, address, former addresses,

and former and current employers – to government agencies.

Rights of Consumers

The FTC has developed “A Summary of Your Rights” under the FCRA regarding collection and dissemination of consumers’ sensitive financial data. (See sidebar below.) Consumer reporting agencies must delete or correct inaccurate, incomplete, or unverifiable information and may not report outdated negative information. Violators may be subject to damages by consumers, and additional rights are provided to victims of identity theft.

There are a number of civil sanctions available when FCRA violations occur. The statute allows for damages to be assessed against actors who are in “willful” or “negligent noncompliance” with FCRA; however, “good faith” is a complete defense for wrongful disclo-

Uses of Consumer Reports and Consumer Rights under FCRA

Consumer reports may be used to:

- Find out whether a person is subject to a court order or grand jury subpoena
- Gain an extension of credit for the consumer
- Hire, fire, or promote
- Underwrite insurance
- Determine eligibility for licenses or other government benefits as required by law
- Determine child support

Consumer rights under FCRA include ...

- Being told if information contained in your consumer record has been used against you
- knowing what is in your file
- The right to ask for a credit score
- The right to dispute incomplete or inaccurate information that appears in your report
- Unlimited access to your file
- Ability to limit “prescreened” offers of credit or insurance based on credit review

sure. CRAs may be assessed actual damages to the consumer in amounts of \$100 to \$1,000. Likewise, any person who obtains a report under false pretenses may be liable for actual damages to the consumer or \$1,000, whichever is greater. Consumers may also sue for punitive damages and may be awarded attorney's fees if the case is won.

The FCRA also contains criminal sanctions. Any consumer reporting agency officer or employee who knowingly and willfully provides consumer information to an unauthorized person may be fined, or imprisoned for up to two years, or both. Similar penalties apply to persons who obtain consumer report data under false pretenses.

FACTA's Additional Protections

FACTA maintained all of the existing FCRA protections and added new consumer protections, most particularly relating to identity theft. FACTA amended the FCRA by requiring that a CRA who has placed a file on fraud alert at the direction of the consumer must alert all of the other CRAs of the alert (the "one-call" fraud alert). Placing a fraud alert allows consumers to receive a free copy of their credit report once within a 12-month period. FACTA required the FTC and banking regulators to develop regulations designed to prevent identity theft and required covered entities to develop internal procedures to identify identity theft. CRAs are required to block any information identified by the consumer as resulting from an alleged identity theft.

FACTA also contained new requirements pertaining to the disposal of consumer report information and records. The Disposal Rule is designed to reduce the risk of consumer fraud and harm created by improper disposal of personally identifiable information, and it broadly applies to "any person that for a business purpose maintains and otherwise possesses consumer information." In addition to the FTC, federal banking regulators and the Securities and

Exchange Commission are granted enforcement authority over the Disposal Rule. The rule covers any information contained in consumer reports as well as information derived from consumer reports (e.g., information used to establish eligibility for credit, employment, or insurance, including employment background, check writing history, insurance claims, residential or tenant history, or medical history). The types of covered entities that must adhere to the Disposal Rule

information, costs versus benefits of different disposal mechanisms, and changes in technology. "Reasonable measures" may include policies that require paper records to be burned, pulverized, or shredded and may include the destruction or permanent erasure of electronic records so that in either case, the information may not be reconstructed or read.

Third parties who provide contractual destruction services are subject to the Disposal Rule, and the covered entity is required to monitor the third party to

For more information about...

- State laws: www.consumer.gov/id-theft/law_laws.htm
- FACTA: frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf
- FCRA: www.ftc.gov/os/statutes/fcrajump.htm
- FTC: www.ftc.gov
- HIPAA: www.hhs.gov/ocr/hipaa/
- CAN-SPAM: www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm
- Disposal Rule: www.ftc.gov/opa/2005/06/disposal.htm
- ARMA International's comments on the Disposal Rule: www.ftc.gov/os/comments/disposal/index.htm
- Privacy Rule: www.ftc.gov/privacy/privacyinitiatives/financial_rule_bus.html
- Gramm-Leach-Bliley Act: www.ftc.gov/privacy/privacyinitiatives/glbact.html

include CRAs, lenders, insurers, employers, landlords, government agencies, mortgage brokers, automobile dealers, attorneys, private investigators, and debt collection agencies.

The Disposal Rule contains a "Standard for Proper Disposal," which stipulates that those who maintain consumer information for business purposes must properly dispose of it and take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. The standard allows covered entities to determine what constitutes "reasonable measures" based upon the sensitivity of the

information. The covered entity, as a matter of due diligence, may have an independent audit conducted to ensure the third party disposes of records appropriately. Likewise, if the disposal company is certified by a recognized trade association or other party, this may count as compliance.

GLB Privacy Rule

FACTA also strengthens the Privacy Rule, enacted by the Gramm-Leach-Bliley Act (GLB), which is designed to thwart identity theft by imposing information safeguarding requirements. The Privacy Rule requires covered entities to

designate responsibility for coordinating the covered entity's information security plan. The designated individual is charged with identifying material risks to security, confidentiality, and the integrity of the personal information being held, as well as designing a program to control risks and evaluating and adjusting the security program regularly by testing and monitoring.

The Privacy Rule covers personal information, such as name, address, e-mail addresses, instant messaging identification, credit card information, "persistent identifiers" such as a customer number, and other customer information.

The FTC's enforcement authority under FCRA is revealed in several recent actions where the FTC imposed GLB safeguards on non-financial institutions as a remedy for their lack of protections for consumer information. In June 2005, BJ's Wholesale Club was required to

establish and maintain a comprehensive information security program, subject to independent audit every two years for the next 20 years for failing to protect their customers' credit and debit card information. The card numbers were stolen and used to make fraudulent purchases.

Petco Animal Supplies was charged in March 2005 for violating its own corporate privacy policy, posted on the company's website, by inadequately securing customer information collected from online transactions. The FTC settlement prohibits Petco from misrepresenting its privacy policy in the future and requires the company to implement a comprehensive information security program with independent audits every two years for the next 20 years. Tower Records was also fined by the FTC for similar violations.

ARMA International provided comments to the FTC when the Disposal Rule was under consideration. ARMA argued in its comments that the rule should contain a requirement that all security policies and procedures be in writing to ensure the safeguarding and confidentiality of the covered information, to protect against any unanticipated threats or hazards to the security or integrity of such information, and to protect against unauthorized access to, or use of, such information that could result in substantial harm to any individual. The existence of a written policy removes ambiguity about what procedures must be followed and what information should be secured. A written policy also serves as a protection to the covered entity against liability in the event of a security breach. ■

Stacey Moye is senior manager of government relations for Smith Bucklin. She can be contacted at smoye@smithbucklin.com.