InformationShield

FACTA: Policy Implications for Business

By David J. Lineman

The Fair and Accurate Credit Transactions Act of 2003 ("FACTA") became law in December, 2003 and added new provisions to the Fair Credit Reporting Act (FCRA). Enforced primarily by the Federal Trade Commission (FTC), FACTA was enacted to address the increasing problem of identity theft and consumer fraud, and adds new consumer rights to protect personal data accuracy and privacy, including limits on information sharing, and disclosure.

Introduction

The increasing problem of identity theft is causing a tangled web between the various organizations that collect and manage personal data on consumer. The consequences of these regulations and the ensuing actions by regulators are likely to have a major impact on the data protection measures of most companies. While FACTA is primarily targeted at agencies that manage and report on consumer credit, the law has some broader provisions that are likely to impact a large number of enterprises. For example, the data destruction provisions of FACTA may potentially impact thousands of organizations. Examples cited in the FTC commentary to the rule include consumer reporting agencies, lenders, insurers, employers, landlords, government agencies, mortgage brokers, automobile dealers, utility companies, telecommunications companies, and others.

In this paper we discuss the various aspects of FACTA that may impact the security and privacy policies and procedures of any organization.

The Importance of Written Policies

How important are written policies to FACTA? The term "policies and procedures" is found at least 17 times in the actual text. An in many cases, having written policies will substantially limit the liability of an organization. For example, in Section § 615, entitled Requirements on users of consumer reports, item (7) the following text is found:

> "Compliance: A person shall not be liable for failure to perform the duties required by this section if, at the time of the failure, the person maintained reasonable policies and procedures to comply with this section."

This same theme is repeated throughout the text of the law.

Data Classification: What data needs protecting?

According to FACTA, organizations should take reasonable measures to protect consumer information throughout the lifecycle of this data. According to FACTA, "Consumer information" is defined as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report." The idea is to protect personally identifiable data, or data which can be associated clearly with one individual. The rule mentions "a variety of personal identifiers beyond simply a person's name…, including, but not limited to, a social security number, driver's license number, phone number, physical address, and e-mail address." In short, many of the data items that corporation use as unique identifiers will end up on this list.

If your organization collects, stores or transmits any of this data, you should consider updating your data classification policies to see if they properly address protection of consumer data. (In the March 2005 Issue of the Policy Solutions Newsletter we discussed data classification policies.)

Some questions to consider:
1. Do our data classification policies provide appropriate sensitivity classifications for consumer data that may impact their credit report?
2. Are data owners training on procedures for identifying sensitive consumer information?
3. Do our policies specify time frames and procedures for data de-classification?
4. Do classification labels follow date throughout its lifecycle, including disposal and destruction?

Red Flags: Prevention as well as detection

According to FACTA, credit reporting agencies must adopt procedures designed to prevent identity theft before it occurs. Certain events such as a change of address or a request for a replacement credit card, in combination with other data, may signal a potential fraud. Consumers who notify a credit agency that they might be the victim of identity theft are granted special provisions, including a "red flag" or marker on their file. While there are currently no official guidelines on specific procedures, FACTA requires Federal agencies to publish guidelines for this type of detection, similar to the intra-

agency guidelines for enforcing the Privacy and security provisions of the Gramm-Leach-Bliley Act (GLBA).

With identity theft as one of the fastest growing crimes, it is a good idea for any organization that deals with customer data to begin thinking about this problem. Organizations should look to see what types of policies and procedures can be enacted to help reduce the chance of an accidental loss of customer data.

Some questions to consider:

1. Does our organization provide training to employees on identity theft?
2. Do we have written policies and procedures for identifying possible identity theft incidents in our own data?
3. Are there any internal data integrity controls that might be used to prevent or detect the theft of our customer data?
4. What technical controls could we use to implement these "red flag" provisions? (For example, database triggers or audit log monitoring.)

Consumer Request Policies

Another element of FACTA reflects a growing trend in privacy-related laws – responding to consumer requests. Many privacy laws, such as HIPAA and the EU Data Protection Directive are based on the "Fair Information Principles" developed by the OECD. Once of the key principles of privacy is the consumer's right to examine their data records for accuracy.

Previously, disputes about the accuracy of information in a consumer report had to be made directly to the consumer reporting agency. Under new FACTA provisions, a consumer may dispute inaccurate information directly with a "furnisher," that is, a creditor that submits data to the credit agency. Upon notice of disputed information, the furnisher must investigate and provide a timely response to the inquiry (usually within 30 days) and cannot report negative information while the investigation is pending.

If your organization is handling personally identifiable consumer data, you should already be considering a set of internal policies and procedures for handling consumer requests to validate the accuracy of this information, including the security and privacy requirements of this process.

Some questions to consider:

1. Do we have a formal written policy for responding to customer requests to validate their personal information?
2. Do we have an individual, or group of individuals responsible for responding to customer inquiries about their personal data?

3. Do we notify our customer, both in print and on-line interactions, that they have the right to examine their personal data?
4. Does the organization have documented policies and procedures for protecting customer information during these transactions?

Consumer Notification

A new provision of FACTA is that consumers are to receive notification prior to or within 30 days of "negative" information being reported to a credit bureau. While this may only apply to organizations that report to credit bureaus, the issue of consumer notification in the event of a possible breach of information is becoming much larger.

For example, California Senate Bill 1386 requires organizations that experienced a security breach to notify individuals who might be affected by the loss of data. In some cases, organizations have elected to notify individuals even though they were not required to do so. Recent rulings by the FTC and other federal agencies indicate that this might become a standard practice for responding to security breaches that may disclose personally identifiable information.

Some questions to consider:

1. If our organization handles sensitive personal information of consumers, do we have a written policy that describes if consumers will be notified?
2. Do we have internal procedures and techniques for rapidly contacting a large segment of our customer base?
3. Do we have written guidelines that describe what types of security incidents may trigger a customer notification?
4. If we handle data that may be reported to a credit agency, will we be able to respond to such a request within 30 days?

Employment Policies and Procedures

One of the best places to begin a solid personnel security program is within the hiring process. Many corporations have hiring policies that require drug screening, credit checks or background checks, especially for key positions within the organization. Employment and hiring policies and procedures are another area to review for FACTA implications.

FACTA makes it clear that medical records are a large concern with respect to data privacy. This linking came from a Federal Reserve Board study that showed that a large percentage of credit report entries had to do with medical claims, and in many of these listings it was possible to discern a medical condition from the record. According to FACTA, companies must

obtain written consent from a potential or current employee before obtaining their medical records.

The request of credit information from potential employers is talked about at length in FACTA. According to § 613, when a credit organization receives a credit report in response to an application for employment, the organization must notify the individual that may be effected by the data in the report, including the name of the entity requesting the information. The law also stipulates that hiring organizations should provide clear notification to potential or current employees that their credit data may be obtained.

Some questions to consider:
1. Do we have a clearly documented set of pre-employment policies that we can give to prospective employees?
2. If we obtain personal medical or credit information, is this clearly articulated and acknowledged by the potential employee?
3. If we obtain personally sensitive data, do we have procedures in place to protect this during the collection, storage and destruction process?
4. Do our employees clearly understand what data we may obtain about them and how it is protected?

Data Destruction Policies

Section 216 of FACTA required the Federal Trade Commission ("FTC") and other federal agencies to issue regulations governing the disposal of consumer credit information. The FTC final rule becomes effective June 1, 2005, and creates broad responsibilities for companies that use or handle information subject to the rule.

The stated purpose of the rule is to "reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information." This purpose is articulated in the section 682.3(a) standard of the rule:

> *Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.*

The proper disposal of sensitive corporate data has become a large topic for many enterprises. Many identity-theft crimes are achieved by "dumpster diving" or pulling data from discarded equipment that was supposedly scrubbed. In the commentary to the rule, the FTC makes it clear that these same protective measures also apply to data destruction service providers.

Some questions to consider:

1. Do we have clearly documented data destruction policies?
2. Are employees training on the proper destruction of various classes of information?
3. Do our data destruction policies include the potential role of 3rd party disposal services?
4. Is the protection of personal data documented in written job descriptions for employees that interact with this data?

For organizations that need help with data classification and destruction policies, *Information Security Policies Made Easy* by Charles Cresson Wood provides many pre-written samples that cover these topics and many other key security concerns.

Penalties for non-compliance

Organizations who are found to have willfully violated the provisions of FACTA (Section § 616) are liable for actual damages sustained to each individual effected as a result of the violation, plus additional court-determined punitive damages and attorney fees. The Federal Trade Commission will be the primary enforcement agency for FACTA. However, as with GLBA, other federal agencies such as the Federal Reserve Board and the National Credit Union Association (NCAU) with jurisdiction over various financial entities will also play a role.

Summary

While FACTA is primarily targeted at organizations that handle financial and credit data of individuals, it has several provisions that may impact a large number of organizations. FACTA provisions illustrate several important trends in information security and privacy, and organizations should consider assessing their security policies and procedures against these as “leading practices” to protect consumer data. What laws and recent rulings have indicated is that the Federal Government is very concerned about the privacy of individuals, and is increasingly taking action to support this position. Yet many companies must collect this type of data to in order to do business. In order to avoid an embarrassing and costly incident, organizations must get serious about how they collect, store, transmit and destroy this sensitive data.

About the Author

David Lineman is President and CEO of Information Shield. Mr. Lineman has 20 years of experience in software development, business consulting and security. He is a frequent speaker and author on the subjects of security policy and regulatory requirements.

References

[1] The Fair Credit Reporting Act (as amended by FACTA): November 2004 – Federal Trade Commission [http://www.ftc.gov/os/statutes/031224fcra.pdf]

[2] OECD Fair Information Principles – Organisation for Economic Co-operation and Development - Published by the OCD [http://www.oecd.org/]

[3] Gramm-Leach-Bliley Act, Title V – Federal Trade Commission. Also published in the Federal Registrar. [http://www.ftc.gov/privacy/glbact/]

[4] Information Security Policies Made Easy, by Charles Cresson Wood. Published by Information Shield, Inc. 2002-2004. [http://www.informationshield.com]

[5] Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood. Published by Information Shield, Inc. 2002-2004. [http://www.informationshield.com]

[6] Health Insurance Portability and Accountability Act of 1996 (HIPAA): Final Security Rule. Department of Health and Human Services; Published in the Federal Registrar. [http://aspe.hhs.gov/admnsimp/index.shtml]

About Information Shield - Information Shield is a global provider of security policy solutions that enable organizations to effectively comply with international regulations. Information Shield products are used by over 7000 customers in 59 countries worldwide. Find out more at our Regulatory Resource Center at www.informationshield.com or contact the author at dave@informationshield.com

informationshield.com

2660 Bering Drive Houston, TX 77057 TEL 1.888.641.0500 FAX 713.783.5365