Order Code RS22087
Updated May 17, 2005

CRS Report for Congress

Information Brokers: Federal and State Laws

Angie A. Welborn
Legislative Attorney
American Law Division

Summary

Media reports concerning the theft of a number of files from major information brokers (also known as data brokers or data merchants), such as ChoicePoint, have brought consumer information privacy to the forefront of the congressional agenda. While there are currently no federal laws specifically related to the information gathering and brokerage industry, there are federal laws that could be applicable depending on the type of information in question and the character of the organization collecting and disseminating the information. This report discusses the federal and state laws that could be applicable to information brokers and legislation that has been introduced to address consumer concerns about the practice of information gathering, the selling of consumer information, and identity theft resulting from security breaches (S. 115, S. 500, S. 751, S. 768, H.R. 1080). The report will be updated as events warrant.

Introduction

In February 2005, ChoicePoint announced that approximately 145,000 records had been improperly disclosed due to fraudulent information presented to ChoicePoint by a purchaser of its information services.[1] ChoicePoint made the announcement only after it was reported that the company had disclosed to residents of California that their information may have been compromised. While several states have recently enacted laws addressing security breaches, there are no federal laws that specifically relate to the information brokerage industry. However, there are other federal laws that could be

[1] For a detailed description of how the fraud was committed, see Robert O'Harrow, Jr. *ChoicePoint Data Cache Became a Powder Keg*. Washington Post. March 5, 2005.

applicable to information brokers[2] depending on the type of information in question and the character of the entity collecting and disseminating the information.

Federal Laws

There are currently no federal laws specifically related to information brokers, nor is there a specific federal law that governs all uses of consumer information. There are several statutes and regulations that restrict the disclosure of consumer information and require entities that collect consumer information to institute certain procedures to insure the security of the information. These laws may be applicable to information brokers depending on the nature of the information they collect and disseminate and the character of the brokerage company. The laws specifically related to the security of consumer information are discussed below.[3]

Fair Credit Reporting Act

Under the Fair Credit Reporting Act (FCRA), consumer reporting agencies have particular responsibilities with respect to ensuring that a consumer's information is used only for purposes that are permissible under the act, for protecting the consumer's information from potential identity thieves, and for correcting information in a consumer's report that may be incorrect or the result of fraud.[4] The act and the requirements set forth therein only apply to entities that fall within the definition of a "consumer reporting agency," and only to products that fall within the definition of a "consumer report."

The FCRA defines "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing

---

[2] S. 500 and H.R. 1080, discussed *infra*, define "information broker" as "a commercial entity whose business is to collect, assemble, or maintain personally identifiable information for the sale or transmission of such information or the provision of access to such information to any third party, whether such collection, assembly, or maintenance of personally identifiable information is performed by the information broker directly, or by contract or subcontract with any other entity." For background on information brokers (or data brokers), see CRS Report RS22137, *Data Brokers: Background and Industry Overview*.

[3] Two other laws applicable to other types of information are not discussed in this report. The Driver's Privacy Protection Act (18 U.S.C. 2721 - 25) prohibits state motor vehicle departments from disclosing personal information in motor vehicle records, subject to certain exceptions. Under rules promulgated pursuant to the Health Insurance Portability and Accountability Act (45 C.F.R. Part 164), entities must take certain steps to ensure the privacy of medical records and are prohibited from disclosing certain information without the consent of the patient.

[4] 15 U.S.C. 1681 *et seq.* For a detailed discussion of the requirements imposed under the Fair Credit Reporting Act, see CRS Report RL31666, *Fair Credit Reporting Act: Rights and Responsibilities*.

consumer reports."[5] Information brokers are arguably consumer reporting agencies within the context of the act as they do assemble and evaluate consumer credit and other information, and subsequently provide this information to third parties. However, even if the brokers may perform the same or similar functions as consumer reporting agencies, the products they provide must be consumer reports in order for the provisions set forth in the FCRA to be applicable.

A "consumer report" is defined under the act as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under section 604 [of the FCRA]."[6] Information brokers have acknowledged that some of the products they provide are consumer reports. However, other data products, that are not used for any of the purposes outlined in the FCRA, are not consumer reports and are not subject to the protections afforded under the act.

Gramm-Leach-Bliley Act

Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) prohibits financial institutions from sharing nonpublic personally identifiable customer information with non-affiliated third parties without giving consumers an opportunity to opt out. The act requires financial institutions to provide customers with notice of their privacy policies, and requires financial institutions to safeguard the security and confidentiality of customer information.[7] The requirements set forth in the act apply to "financial institutions," which are defined as "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956."[8] These activities include those that are traditionally associated with banking, as well as activities such as credit reporting. If an information broker were engaging in consumer reporting activities, as discussed above, they could also fall within the definition of a financial institution for purposes of GLBA.

Should information brokers fall within the definition of a financial institution under GLBA, they could be subject to both the privacy rule[9] and the safeguard rule.[10] If an information broker receives information from a credit reporting agency, they may also be

---

[5] 15 U.S.C. 1681a(f). The act also defines "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" and "nationwide speciality consumer reporting agency."

[6] 15 U.S.C. 1681a(d). The act also defines "investigative consumer report."

[7] P.L. 106-102. For more information on the requirements imposed under GLBA, see CRS Report RS20185, *Privacy Protection for Consumer Financial Information.*

[8] 15 U.S.C. 6809(3)(A). Section 4(k) of the Bank Holding Act is codified at 12 U.S.C. 1843(k).

[9] 12 C.F.R. 225.28, 225.86

[10] 16 C.F.R. Part 314.

limited by GLBA's reuse and redisclosure provisions, which could limit the broker's use of that information.

State Action

In 2002, California enacted a law requiring a state agency, or any person or business that owns or licenses computerized data that includes personal information to disclose any breach of security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[11] The disclosure must be made in the "most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[12]

Following the announcement by ChoicePoint and other high profile cases involving information brokers, legislation was introduced in several other states. Georgia recently enacted a law similar to the California law discussed above.[13] While the California law covers any person or business, including a state agency, the Georgia law applies only to "information brokers," which is defined to specifically exclude governmental agencies.[14] Arkansas,[15] Indiana,[16] Montana,[17] North Dakota,[18] and Washington[19] have enacted similar laws requiring notification by either business or state agencies, or both. Several other states are considering such legislation.[20]

Congressional Response

S. 115, the **Notification of Risk to Personal Data Act**, was introduced prior to the incidents involving ChoicePoint and other information brokers. The bill, similar to the California law discussed above, would require "any agency, or person engaged in interstate commerce, that owns or licenses electronic data containing personal information" to "notify any resident of the United States whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized

---

[11] SB 1386, codified at Cal. Civ. Code 1798.29 and 1798.82.

[12] Cal. Civ. Code 1798.29(a); 1798.82(a).

[13] SB 230, to be codified at O.C.G.A. 10-1-910 *et seq.*

[14] O.C.G.A. 10-1-911(2).

[15] Act 1526, 85th General Assembly, Regular Session, 2005.

[16] Senate Bill 503, 114th General Assembly, First Regular Session (2005). The Indiana law appears to apply only to state agencies.

[17] House Bill No. 732, 2005 Montana Legislature.

[18] Senate Bill No. 2251, 59th Legislative Assembly of North Dakota, 2005.

[19] Senate Bill 6043, Chapter 368, Laws of 2005, 59th Legislature, 2005 Regular Session.

[20] For a complete list of pending state legislation, see the National Conference of State Legislatures [http://www.ncsl.org/programs/lis/cip/priv/breach.htm] (last visited May 17, 2005).

person" due to a security breach. Notification would be required "as expediently as possible and without unreasonable delay" following the discovery of the breach of security and any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the integrity of the data system. Notification may be delayed for law enforcement purposes. **S. 751**, also entitled the **Notification of Risk to Personal Data Act** and introduced following the reports of major security breaches, is similar to **S. 115**, but would require notification when any information, whether or not held in electronic form, has been, or is reasonably believed to have been, acquired by an unauthorized person.

S. 500, the **Information Protection and Security Act** was also introduced following the ChoicePoint security breach. The bill would require the Federal Trade Commission to promulgate regulations "with respect to the conduct of information brokers and the protection of personally identifiable information held by such brokers." Such regulations must include a requirement that procedures for the collection and maintenance of data guarantee maximum possible accuracy of the information held by brokers; access by a consumer to information pertaining to him held by an information broker; a consumer's right to request and receive prompt correction of errors in information held by an information broker; a requirement that brokers safeguard and protect the confidentially of information; a requirement that brokers authenticate users before allowing access to information and that the broker ensure that the information will only be used for a lawful purpose; and a requirement that broker's establish procedures to prevent and detect fraudulent or unlawful access, use or disclosure of information. The regulations would be enforced by the Federal Trade Commission and in actions by state attorneys general. A consumer would also be allowed to bring a private right of action to recover actual monetary loss or up to $1000 in damages, whichever is greater. A companion bill, **H.R. 1080**, was introduced in the House.

S. 768, the **Comprehensive Identity Theft Prevention Act**, includes a number of provisions aimed at preventing identity theft, including the creation of an Office of Identity Theft in the Federal Trade Commission and efforts to protect a consumer's sensitive personal information. With respect to the information brokerage industry, the bill would require the Federal Trade Commission to promulgate regulations to enable the newly created Office of Identity Theft to protect sensitive personal information that is collected, maintained, sold, or transferred by commercial entities, such as information brokers. Information brokers, or data merchants, as defined in the legislation, would be required to register with the Office of Identity Theft, and would be required to follow rules promulgated by the Commission regarding the processes for protecting consumer information. Consumers would be given certain rights, similar to those afforded under the Fair Credit Reporting Act, with respect to their information held by a data merchant, and would be able to correct incorrect information and receive one free report from the data merchant each year. Commercial entities would be required to notify consumers of information breaches, and consumers would be able to have their information expunged from the information broker's records following notification of a security breach.