Order Code RL33005

CRS Report for Congress

Information Brokers: Federal and State Laws

Updated May 5, 2006

Angie A. Welborn
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

Information Brokers: Federal and State Laws

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 in the 109th Congress to address consumer concerns about the practice of information gathering, the selling of consumer information, and identity theft resulting from security breaches. The report will be updated as events warrant.

Contents

Information Brokers: Federal and State Laws

Introduction

In 2005, a number of incidents were reported regarding the security of personal information held by information brokers, financial institutions, private businesses, and public entities.[1] Information such as Social Security numbers, names, addresses, medical records, and financial information was compromised and, in some cases, used to commit identity theft. 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 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.[3] 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.[4]

---

[1] *See* CRS Report RL33199, *Personal Data Security Breaches: Context and Incident Summaries*, by Rita Tehan.

[2] For background on information brokers (or data brokers), see CRS Report RS22137, *Data Brokers: Background and Industry Overview*, by Nathan Brooks.

[3] For an overview of federal and state laws related to data security, see CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens.

[4] Three 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. Finally, Section 222 of the Communications Act of 1934, as amended (47 U.S.C. 222), establishes a duty of every telecommunications carrier to protect

(continued...)

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.[5] 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 consumer reports."[6] 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]."[7] 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

---

[4] (...continued)
the confidentiality of its customers' customer proprietary network information (CPNI). For more information on the protection of CPNI and telephone record information, see CRS Report RL33287, *Data Security: Protecting the Privacy of Phone Records*, by Gina Marie Stevens.

[5] 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*, by Angie A. Welborn.

[6] 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."

[7] 15 U.S.C. 1681a(d). The act also defines "investigative consumer report."

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.[8] 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."[9] 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[10] and the safeguard rule.[11] If an information broker receives information from a credit reporting agency, they may also be 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.[12] 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."[13]

---

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

[9] 15 U.S.C. 6809(3)(A). Section 4(k) of the Bank Holding Act is codified at 12 U.S.C. 1843(k).

[10] 12 C.F.R. 225.28, 225.86

[11] 16 C.F.R. Part 314.

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

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

Following the reports of a number of 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.[14] 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.[15] Arkansas,[16] Indiana,[17] Montana,[18] North Dakota,[19] and Washington[20] have enacted similar laws requiring notification by either business or state agencies, or both. Several other states are considering such legislation.[21]

Congressional Response

Several bills have been introduced in both houses of Congress in the 109th Congress to address concerns associated with the information brokerage industry and security breaches.[22] To date, committee action has been taken on several of the bills discussed below, but neither house has considered legislation on the floor.

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 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,

---

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

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

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

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

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

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

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

[21] For a complete list of state legislation considered in 2005, see the National Conference of State Legislatures [http://www.ncsl.org/programs/lis/cip/priv/breach.htm] (last visited January 11, 2006).

[22] For an overview of the legislative approaches being considered with respect to information brokers and the broader topic of data security, see CRS Report RL33273, *Data Security: Federal Legislative Approaches*, by Gina Marie Stevens.

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. 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.

S. 1216, the **Financial Privacy Breach Notification Act of 2005**, would amend the Gramm-Leach-Bliley Act to require a financial institution,[23] and any person that maintains personal financial information for or on behalf of a financial institution, to notify its customers, consumer reporting agencies, and law enforcement agencies when there has been a breach of personal financial information. Any customer injured as a result of the institutions' failure to notify would be allowed to bring a civil action to recover damages arising from the failure.

---

[23] As noted above, it is not clear to what extent any particular information broker may fall within the definition of "financial institution" under Gramm-Leach-Bliley. Thus, it is not clear to what extent this requirement would be applicable to information brokers.

S. 1326, the **Notification of Risk to Personal Data Act**, would require any agency (state or federal) or person that owns or licenses computerized data containing sensitive personal information to implement and maintain reasonable security and notification procedures to protect the information from unauthorized access, destruction, use, modification or disclosure. The agency or person would be required to notify any individual, if such individual is known to be a resident of the United States, whose information was compromised in the event of a breach that could result in significant risk of identity theft. Notification would be required to be made as expeditiously as possible, but may be delayed for law enforcement purposes. The legislation prescribes acceptable methods of notice and would require coordination with consumer reporting agencies if more than 1,000 individuals at a time have been affected by a breach.

The Senate Judiciary Committee ordered the bill to be reported without amendment favorably on October 10, 2005.

S. 1332, the **Personal Data Privacy and Security Act of 2005**, includes a number of provisions aimed at preventing identity theft and ensuring the privacy of personally identifiable information. Under the bill, consumers would have rights with respect to the information held by data brokers similar to the rights provided to consumers under the Fair Credit Reporting Act, including the right to have the information disclosed to them and the right to dispute inaccurate information. The bill would also require any business entity or agency engaged in interstate commerce to notify the United States Secret Service, consumer reporting agencies, and any resident of the United States whose information has been compromised in the event of a security breach that impacts more than 10,000 individuals nationwide, impacts a database, networked or integrated databases, or other data system associated with more than 1,000,000 individuals nationwide, impacts databases owned or used by the federal government, or involves sensitive information of employees and contractors of the Federal Government.

S. 1408, the **Identity Theft Protection Act**, would require broadly defined covered entities to take reasonable steps to protect against security breaches and to prevent unauthorized access to sensitive personal information pursuant to regulations promulgated by the Federal Trade Commission. Under the legislation, if a security breach were to occur, the covered entity would be required, if the breach affected more than 1,000 individuals, to report the breach to the FTC, consumer reporting agencies, and the individuals affected. If a breach occurs that affects one or more individuals and there is a reasonable risk of identity theft, the covered entity must notify each individual affected. Notification must be made not later than 90 days after the breach, but may be delayed for law enforcement or homeland security investigations.

The Senate Commerce, Science and Transportation Committee ordered the bill to be reported with an amendment in the nature of a substitute favorably on July 28, 2005. On December 8, 2005, the Committee issued a written report on the bill.[24] Amendments offered and approved would decrease from 90 days to 45 days the

---

[24] S.Rept. 109-203.

amount of time an entity covered by the bill would have to notify consumers about a security breach, prevent the FTC from issuing technology mandates, and provide that the bill does not create a private right of action for consumers. Additional amendments would require that if a breach involves less than 1,000 people, the entity would notify the FTC, but not the customer, and would generally prohibit the sale of Social Security numbers.

S. 1594, the **Financial Privacy Protection Act of 2005**, would amend the Gramm-Leach-Bliley Act to require financial institutions to develop and maintain a customer information security system that includes policies, procedures, and controls designed to prevent any breach with respect to customer information, and to require the notification of customers when there has been a breach. In the event of a breach of security, a financial institution would be required to notify each customer whose information was or is reasonably believed to have been accessed in connection with the breach or suspected breach, the appropriate Federal functional regulator, each nationwide consumer reporting agency, and appropriate law enforcement agencies in cases where the breach affects a large number of customers. Delivery of the notification would be required promptly and without unreasonable delay upon discovery of the breach or suspected breach, but it may be delayed for law enforcement purposes. The notification could be in writing, electronic form, or, if the breach affected more than 500,000 or if the cost of notification would be more than $500,000, in a conspicuous posting on the institution's website and through major media outlets.

S. 1789, the **Personal Data Privacy and Security Act of 2005**, includes a number of provisions related to identity theft, data brokers, and data privacy and security. The bill would require data brokers to make disclosures to individuals similar to those required under the Fair Credit Reporting Act (FCRA) and would allow individuals to dispute inaccurate information through a process similar to that under the FCRA. The legislation would also require covered entities to implement a comprehensive personal data privacy and security program, conduct risk assessments, and design security programs to control identified risks. Employees of those entities would also be required to undergo training for the implementation of the data security program, and business would be required to regularly test security systems and procedures set forth under the data security program. The bill would also require any agency or business entity to notify, following the discovery of a security breach, any resident of the United States whose information was subject to the breach. Notification would be required without unreasonable delay but could be delayed for law enforcement purposes. Depending on the number of individuals affected by the breach, entities may also be required to notify credit reporting agencies, the United States Secret Service, and other federal and state law enforcement agencies. Exemptions from the notification requirement would be available for national security purposes, for entities that are able to assess that no significant risk of harm has resulted from the breach, and for entities that use a security program that is designed to block the use of the information to initiate unauthorized financial transactions.

The Senate Judiciary Committee ordered the bill to be reported with an amendment in the nature of a substitute favorably on November 17, 2005. Apart from the substitute, no other amendments were approved by the Committee.

H.R. 1069, the **Notification of Risk to Personal Data Act**, 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 encrypted personal information was, or is reasonably believed to have been, lost or acquired by an unauthorized person following the discovery of a breach of security of the system containing such data. The entity would also be required to notify consumer reporting agencies of the loss or unauthorized acquisition with respect to such consumer. The bill would also amend the Gramm-Leach-Bliley Act to require financial institutions to notify customers, consumer reporting agencies, the Federal Trade Commission, and law enforcement agencies of breaches involving computerized or paper records.

H.R. 3140, the **Consumer Data Security and Notification Act of 2005**, would amend the Fair Credit Reporting Act to include in the definition of consumer report any written, oral, electronic, or other communication of any information by any person which, for monetary fees, dues or other compensation, regularly engages in whole or in part in the practice of assembling or evaluating personally identifiable information for the purpose of furnishing reports to third parties that include the name of any consumers and certain other information, thus effectively applying the provisions of the FCRA to a broader group of entities. An additional amendment to the FCRA would require consumer reporting agencies to notify consumers following the discovery of a breach of security of any data system maintained by the agency in which sensitive consumer information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would also amend the Gramm-Leach-Bliley Act to require financial institutions to notify customers following a breach of security. A financial institution would also be required to notify its primary federal regulatory agency and the appropriate law enforcement agency of the breach, and take steps to remedy the breach and safeguard the interests of affected customers.

H.R. 3374, the **Consumer Notification and Financial Data Protection Act of 2005**, would require financial institutions to maintain reasonable policies and procedures to protect the security and confidentiality of sensitive financial personal information. The bill defines "financial institution" to include an entity engaged in activities typically associated with financial institutions under the Gramm-Leach-Bliley Act, entities subject to the Fair Credit Reporting Act, and any person that is maintaining, receiving, or communicating sensitive financial personal information on an ongoing basis for the purpose of engaging in interstate commerce, which could arguably include those entities generally referred to as information or data brokers. A financial institution would be required to conduct an investigation whenever it becomes aware of information that would reasonably indicate that a breach of data security may have occurred or is reasonably likely to occur. If, after the investigation, the institution determines that a breach may result in harm or substantial inconvenience to any consumer whose information was involved, the institution would be required to notify law enforcement agencies and the institution's functional regulator, take reasonable measures to ensure and restore the security of the information, take measures to prevent further unauthorized access, and notify all critical third parties whose involvement is necessary to investigate the breach or who will be required to undertake further action to protect consumers from fraud or identity theft. The institution would also be required to notify each consumer whose

information was involved in the breach; and if notice must be provided to more than 1,000 consumers, notice must also be provided to consumer reporting agencies.

H.R. 3375, the **Financial Data Security Act of 2005**, would also amend the Fair Credit Reporting Act to broaden the act's current scope. The amendments would add new definitions classifying entities that engage in information gathering, collection, and dissemination and require such entities to maintain reasonable policies and procedures to protect the security and confidentiality of sensitive financial account information and identifying information of consumers. If such entities are aware that a breach of security has occurred, the bill would require them to conduct an investigation to determine the likelihood that consumer information will be misused. Unless the entity determines that it is not reasonably likely that the information will be misused, the bill would require the entity to notify the appropriate law enforcement agency, the appropriate regulatory agency, any consumer to whom the information relates, and if the notice is to be provided to more than 1,000 consumers, to each nationwide consumer reporting agency. Any entity that is required to provide such notice, must also offer to consumers, free of charge, a service that monitors nationwide credit activity.

H.R. 3997, the **Financial Data Protection Act of 2005**, would amend the Fair Credit Reporting Act to require entities defined as "consumer reporters" to implement and maintain reasonable policies and procedures to protect the security and confidentiality of sensitive financial personal information. Consumer reporters would also be required to investigate any breach of security that has occurred or that is reasonably likely to occur and notify appropriate law enforcement, regulatory, and other entities if the breach is likely to result in substantial harm to consumers. The legislation would require notification of consumers if the consumer reporter becomes aware that a breach of security is reasonably likely to have occurred and that information obtained during the breach is reasonably likely to be misused to commit identity theft or to make fraudulent transactions on such consumers' accounts. The notice provided would generally be required to include a description of the nature and type of information subject to the breach; the date and time of the breach, if known; a general description of the actions taken by the consumer reporter to restore the security and confidentiality of the information; and a toll-free telephone number for obtaining additional information. If the breach involved information defined as "sensitive financial identity information," the notice would also be required to include a summary of rights of victims of fraud or identity theft, including information on how to obtain a free credit report, how to place a fraud alert in the consumer's file, and instructions for obtaining file monitoring mitigation. A substantially similar bill, **S. 2169**, was later introduced in the Senate.

On March 16, 2006, the House Committee on Financial Services considered H.R. 3997 and ordered the bill to be reported with amendments. Of the amendments approved were those that would require the GAO to study how to create a data breach notification system for those who speak languages other than English, that would require the FTC compile information on the race and ethnicity of identity fraud victims, and that would require the FTC assemble a public list of data security breaches for the last year, including information on the company responsible for the breach and a general description of the case.

H.R. 4127, the **Data Accountability and Trust Act (DATA)**, would require the Federal Trade Commission to promulgate regulations to require each person engaged in interstate commerce that owns or possesses data in electronic form containing personal information to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information. Entities defined as information brokers would be required to submit their information security policies to the Commission on an annual basis and would be subject to audits by the Commission following a breach of security. Pursuant to the legislation, information brokers would also be required to allow individuals to have access to their personal information on file with broker and to dispute inaccurate information. The bill would also require notification to each individual of the United States whose personal information was acquired by an unauthorized person as the result of a breach of security. Notification must also be provided to the Commission and, in the case of a breach of financial account information, to the financial institution that issued the account. Substitute notification, in the form of notice to print and broadcast media outlets, would be allowed if direct notification is not feasible due to excessive cost or lack of sufficient contact information.

Following a markup by the Subcommittee on Commerce, Trade and Consumer Protection, the House Committee on Energy and Commerce considered H.R. 4127 on March 29, 2006, and ordered the bill to be reported with amendments. The manager's amendment approved by the full committee included language that would change the threshold for notifying consumers of a security breach — from when such a breach poses a "significant risk" of identity theft or other fraud for the affected consumers to a "reasonable risk" of such problems. The amendment also would allow for enforcement of the bill's provisions by state attorneys general in addition to the FTC, prohibit data brokers from obtaining information about a consumer by impersonating the person (a practice known as pretexting), and allow consumers annual access to information about them and the opportunity to correct inaccurate data.