THE GRAMM-LEACH-BLILEY ACT: FIVE YEARS AFTER IMPLEMENTATION, DOES THE EMPEROR WEAR CLOTHES?

KATHLEEN A. HARDEET†

INTRODUCTION

Five years ago, the Gramm-Leach-Bliley Act was fervently debated and unveiled to the public with more pomp and circumstance than most legislation in recent years. The Act was initially touted to be both an economic boon to financial institutions and a revolutionary step in the protection of consumer privacy in this generation of computers and technical data sharing. Now, five years after its implementation,¹ a review of the performance of the Gramm-Leach-Bliley Act is warranted to evaluate performance to date and expectations for the future.

I. PURPOSE AND CREATION

What was ultimately sold to the public as an effort by Congress to protect consumers' personal and confidential financial information, the Gramm-Leach-Bliley Act (the "GLBA" or the "Act") initially did not include or even consider the issue of privacy.² The business purpose of the GLBA, also known as the Financial Services Modernization Act of 1999, was "to enhance competition in the financial services industry" by allowing financial services industries to affiliate with one another and to allow those affiliated institutions to share confidential customer data.³ Congress believed that this affiliating and sharing of information would allow financial institutions to better compete both against one another and also throughout the world. This competition would in turn benefit consumers both by increasing the availability of financial products and services and also by favorably impacting pricing.⁴ Hypothetically, the net cost to consumers would decrease due to the ready access affiliated entities would have to customers' personal

† Shughart, Thomson & Kilroy, P.C.
and financial information. To implement this business purpose, the GLBA first had to repeal sections of the Glass-Steagall Act, a New Deal regulation that had previously restricted affiliations between commercial banks and securities firms.

On May 6, 1999, the Senate gave approval to Senate Bill 900, which was the initial version of the Act, sans any consideration of privacy concerns. It was at that point that the mechanism created to benefit financial institutions became a lightning rod for consumers' fear of their increasing loss of privacy in an electronically integrated world. The House Commerce Committee was the first to question the absence of any safeguards in the bill to protect the shared information, which would now be flowing between affiliates. The Committee proposed to impose upon financial institutions an obligation to create "procedures to protect the confidentiality and security of nonpublic personal information collected in connection with any transaction of their customers." The concept proved to be easier in the abstract than in the definition. Ultimately the House Committee defined "nonpublic personal information" in the negative as "personally identifiable information, other than publicly available directory information, pertaining to an individual's transactions with a financial institution."

And thus the debate began. The financial industry petitioned to narrow their responsibilities by narrowing the definition of "nonpublic personal information." Each layer of safeguards was seen as an impediment to accomplishing the initial goal of the GLBA, to facilitate the free flow of information. What had begun as a measure to permit the sharing of more information among financial affiliates was now developing into a scheme the financial services industry feared would actually impede their ability to use that shared information.

On the other side of the debate, privacy proponents sought a broader definition of "nonpublic personal information." In doing so, they sought protection of more than just a consumer's transactions with a financial institution. Some advocated, and ultimately pre-

---

8. Id. at 94.
vailed in including within the bill, protection of social security numbers, account applications, and account histories. Others' arguments for including personal medical information that is shared in the context of financial services transactions ultimately failed.

Beyond the threshold definition of "nonpublic personal information," legislators debated what procedures ought to be used to appropriately protect the personal information that would now be shared between affiliates. While the GLBA presumes that nonpublic personal information will be freely shared between affiliated entities, the question arose as to what limitations should be imposed to protect that information from being disseminated to nonaffiliated entities.

After extensive debate, President Clinton signed into law the final version of the Gramm-Leach-Bliley Act on November 12, 1999. Tucked in at the end of the Act was the ultimate compromise arising from the debates regarding privacy considerations. That policy is best summarized in the opening provisions of Subtitle A of Title V of the Act:

§ 6801. Protection of nonpublic personal information

(a) Privacy obligation policy
It is the policy of the congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial institutions safeguards
In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.
The threshold definitional issue of who is included within the scope of the term "financial institution" was addressed in §6805(a). In that section the following entities, and those subject to their jurisdiction, were intended to be subject to the privacy protections of the GLBA:


b. "[M]ember banks of the Federal Reserve System, branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act, and bank holding companies and their nonbank subsidiaries or affiliates" subject to the jurisdiction of the Board of Governors of the Federal Reserve System pursuant to 12 U.S.C. § 1818;14

c. "[B]anks insured by the Federal Deposit Insurance Corporation, insured State branches of foreign banks, and any subsidiaries of such entities" subject to the jurisdiction of the Board of Directors of the Federal Deposit Insurance Corporation pursuant to 12 U.S.C. § 1818;15

d. "[S]avings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations" subject to the jurisdiction of the Director of the Office of Thrift Supervision pursuant to 12 U.S.C. § 1818;16

e. Federally insured credit unions and any subsidiaries of such entities subject to the jurisdiction of the Board of the National Credit Union Administration pursuant to 12 U.S.C. § 1751, et seq.;17

f. Brokers and dealers subject to the jurisdiction of the Securities and Exchange Commission pursuant to 15 U.S.C. § 78a, et seq.;18

g. Investment companies subject to the jurisdiction of the Securities and Exchange Commission pursuant to 15 U.S.C. § 80a-1, et seq.;19

---

h. Registered investment advisors subject to the jurisdiction of the Securities and Exchange Commission pursuant to 15 U.S.C. § 80b-1, et seq.;\(^\text{20}\)

i. “[A]ny person engaged in providing insurance” subject to “the applicable State insurance authority of the State in which the person is domiciled” pursuant to State insurance law;\(^\text{21}\)

j. Any other financial institution not within the parameters of any other provision but subject to the jurisdiction of the Federal Trade Commission pursuant to 15 U.S.C. § 41, et seq.\(^\text{22}\)

After describing policy and defining applicability, Congress went on to outline a procedure for protecting personal information. Such outline is found in 15 U.S.C.A. §6802. In that section the GLBA states that a financial institution may not disclose any nonpublic personal information to any nonaffiliated third party, unless an opt-out notice is provided to the consumer.\(^\text{23}\) The opt-out notice must be given initially when the customer relationship is created, followed by annual privacy notices in each year in which the customer relationship continues. These notices must disclose the types of nonpublic personal information the financial institution collects, as well as the types of information that the financial institution discloses to third parties. If nonpublic personal information is to be disclosed to third parties, the financial institution must then also give its customer an “opt-out” that clearly informs the customer of his or her right to elect to keep personal information private. In connection with business conducted over the Internet, these notices may be given electronically. Certain narrow exceptions from the notice and opt-out requirements are also detailed in the regulations.\(^\text{24}\) Unless the appropriate notices are given and an opt-out opportunity is provided, “financial institutions” may not share or disclose any nonpublic personal information about a consumer or customer.\(^\text{25}\)

II. IMPLEMENTATION

Beyond the general parameters set forth in the GLBA, Congress delegated compliance details to various administrative agencies charged with monitoring financial institutions. The specified agencies, including “the Federal functional regulators, the State insurance

authorities, and the Federal Trade Commission,\textsuperscript{26} were directed to implement and enforce the GLBA.\textsuperscript{27} Although other agencies would later be designated as Federal functional regulators,\textsuperscript{28} the initial agencies charged with responsibility for implementation and enforcement of the GLBA included the Federal Reserve Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Commission (FDIC), the Department of Treasury Office of the Comptroller of the Currency (OCC), the Department of Treasury Office of Thrift Supervision (OTS), National Credit Union Association (NCUA), Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC). At the state level, insurance authorities grappled with the complexity of coordinating both among the states and with the federal system.

Beyond the Act's statement of policy, Congress gave little guidance to the agencies charged with implementing the Act. The agencies were directed to prescribe "such regulations as may be necessary to carry out the purposes of this subchapter with respect to the financial institutions subject to their jurisdiction."\textsuperscript{29} The implementing agencies were further directed to coordinate with one another to assure that "the regulations prescribed by each such agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities."\textsuperscript{30} The only real specific instruction provided by Congress was that the financial institutions subject to the jurisdiction of these agencies must be in full compliance with the Act and notice provisions must be delivered to consumers by July 1, 2001.\textsuperscript{31}

A. State Insurance Implementation

The Gramm-Leach-Bliley Act directed that the federal bank and thrift regulatory agencies work with the National Association of Insurance Commissioners in an effort to coordinate a uniform state approach to the implementation and enforcement of the GLBA.\textsuperscript{32} As directed, on September 26, 2000, the National Association of Insurance Commissioners, together with the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision adopted a model rule, "Privacy of Consumer Financial and

\textsuperscript{28} See infra Section II.B.4.
Health Information Regulation” (“2000 Model Regulation”). This model rule was provided to the state insurance commissioners and became effective November 13, 2000, coinciding with the effective dates of the regulations being issued by the other federal agencies participating in the same process.

In addition to state insurance commissioners, many states legislatures became involved and passed their own privacy provisions more restrictive than the GLBA and, in fact, more protective than the GLBA. The thrust of many state versions went so far as to require state financial institutions to obtain an affirmative consent from the consumer to disclose personal information, even to an affiliate; a type of “opt-in” rather than an “opt-out.” The success of these state programs, in comparison to the federal GLBA efforts, has prompted discussions and suggestions that federal agencies follow suit.

B. FEDERAL IMPLEMENTATION

1. Banking Agencies’ Implementation

While the seven federal agencies were trying to coordinate their efforts, the four banking and thrift agencies assumed the task of adopting joint implementing regulations for their members. These agencies, the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision, regulate very similar entities, including the following: a) national banks, federal branches, and federal agencies of foreign banks and any subsidiaries of such entities; b) member banks of the Federal Reserve System, branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, bank holding companies and their non-bank subsidiaries or affiliates; c) banks insured by the Federal Deposit Insurance Corporation, insured State branches of foreign banks, and any subsidiaries of such entities; and d) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations.

While the similarity of their jurisdictions created the need for consistency in their guidelines, the difficulty of coordinating an inter-agency agreement within multiple federal agencies soon became
The agencies first published preliminary guidelines, referred to as Year 2000 Safety and Standards Guidelines.\textsuperscript{36} Thereafter, the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness were published for comment and were thereafter debated between the agencies until the joint final rule was published in the Federal Register on February 1, 2001, to become effective by the Congressional deadline of July 1, 2001.\textsuperscript{37}

While the guidelines were jointly adopted, each member agency issued its own separate regulations implementing the GLBA, in substantively identical texts.\textsuperscript{38} Each of the banking agencies' regulations were effective as of November 13, 2000,\textsuperscript{39} and each required notices to be served upon consumers by July 1, 2001.\textsuperscript{40} In addition to separate regulations, several agencies issued separate publications to their member financial institutions. On January 26, 2001, the FDIC issued a Privacy Rule Handbook to "help banks, particularly smaller banks, meet their obligations under the privacy rule" of the GLBA.\textsuperscript{41}

2. NCUA Implementation

Because the National Credit Union Administration (NCUA) chose not to issue its regulations jointly with the banking and thrift agencies, its process of drafting and publishing regulations occurred more swiftly. The NCUA published the final version of its regulations implementing the GLBA at 12 C.F.R. Part 716 on May 18, 2000, nine months before the interagency regulation was negotiated. The NCUA's implementing regulation became effective on November 13, 2000,\textsuperscript{42} with compliance required by July 1, 2001.\textsuperscript{43} Although NCUA's regulations are substantially similar to the Interagency Guidelines adopted by the banking agencies, the NCUA particularly

\textsuperscript{36} Year 2000 safety and soundness standards were applicable to insured depository institutions pursuant to section 39 of the Federal Deposit Insurance Act ("FDI").


\textsuperscript{42} 12 C.F.R. § 716.18(a) (2000).

\textsuperscript{43} 12 C.F.R. § 716.18(b)(1) (2000).
tailored its regulations to the terminology and structure of credit unions and established specific duties and limitations for credit union members based on their activities.\textsuperscript{44}

3. \textit{SEC Implementation}

The SEC initially believed that it would not be necessary to prepare any implementing regulation at all. The implementation and enforcement provisions of 15 U.S.C.A. § 6804(a)(1) do not require that implementing regulations be developed, but only "such regulations as may be necessary to carry out the purposes of this subchapter with respect to the financial institutions subject to their jurisdiction."\textsuperscript{45} The SEC anticipated that it had the necessary structures in place to be able to enforce the GLBA without drafting any implementing regulations. Ultimately, the Commission received sufficient feedback to convince it that some direction was necessary, and it assumed the task of drafting implementing regulations.\textsuperscript{46}

On June 29, 2000, the SEC issued Regulation S-P, "Privacy of Consumer Financial Information," which specifically makes the GLBA privacy requirements applicable to brokers, dealers, and investment companies whether or not they are registered with the SEC, as well as to investment advisors registered with the SEC under the Investment Advisors Act of 1940.\textsuperscript{47}

4. \textit{CFTC Implementation}

As originally drafted, Congress specifically excluded the Commodity Futures Trading Commission (CFTC) from the requirements of the GLBA. The exclusion in 15 U.S.C.A. § 1609(3)(B) provided that notwithstanding any other provisions of the Act, "the term ‘financial institution’ does not include a person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act [7 U.S.C. §1, et seq.]."\textsuperscript{48} The exclusion was eliminated on December 21, 2000, with the enactment of the Commodity Futures Modernization Act.\textsuperscript{49} This new law served to amend the Commodity Exchange Act to

---

\textsuperscript{44} Letter from National Credit Union Administration to Federally Insured Credit Unions (Feb. 2002), available at http://www.ncua.gov/letters/2002/02-CU-02.html.


\textsuperscript{47} 17 C.F.R. § 284.10.


include the CFTC as a federal functional regulator within the meaning of Title V of the GLBA,\(^5\) to include CFTC members as financial institutions within the meaning of the GLBA,\(^5\) and to require the CFTC to prescribe the requisite regulations that would become effective within six months.\(^5\)

While the other federal implementing agencies had eighteen months from the date the GLBA was adopted until its regulations had to be implemented, the CFTC had only six months. The CFTC coordinated with the other agencies, and in particular the SEC, but in the end, six months proved to be an unrealistic demand. Advising CFTC members of a change in policy and adopting and implementing regulations could not be accomplished in six months. The CFTC issued its regulations implementing the GLBA effective June 21, 2001,\(^5\) and requiring its financial institutions to provide notice to consumers no later than March 31, 2002.\(^5\)

5. **FTC Implementation**

No agency's responsibilities under the Act were broader than those of the FTC, given the catch-all responsibility of implementation and enforcement for "[a]ny other financial institution" not within the parameters of any other provision but subject to the jurisdiction of the Federal Trade Commission pursuant to 15 U.S.C. § 41, et seq.\(^5\) The FTC ultimately implemented sweeping regulations, which have commonly been referred to as the "Financial Privacy Rule," "Pretexting procedures," and the "Safeguards Rule."

On May 24, 2000, the FTC approved its Privacy Rule.\(^5\) The Financial Privacy Rule defined "financial institutions" subject to the privacy requirements of the GLBA as "any institution the business of which is engaging in financial activities as described in § 4(k) of the Bank Holding Company Act of 1956"\(^5\) and that governed the collection of personal, confidential financial information received from a consumer during the course of a financial transaction. Additionally, the Financial Privacy Rule also set forth the FTC's procedures for providing customers notice of their rights. The Privacy Rule became effective on November 13, 2000\(^5\) and required that all notices be served

50. 7 U.S.C.A. § 7b-2(b).
57. 16 C.F.R. § 313.3(k)(1) (2000).
58. 16 C.F.R. § 313.18(a) (2000).
upon consumers no later than July 1, 2001.\textsuperscript{59} By way of additional explanation, the FTC issued its own Financial Privacy Guidance outlines for financial institutions under its jurisdiction.\textsuperscript{60}

Further regulations were issued by the FTC implementing the GLBA, including its Pretexting provisions and Safeguards Rule.\textsuperscript{61} Those regulations forbid obtaining confidential information by way of fraudulent means. The regulations further require all financial institutions to create and maintain physical, technical, and procedural system safeguards that operate to protect consumer information, whether that information was received directly or from another financial institution.\textsuperscript{62}  

6. Challenges to Implementation

The unwieldy task of drafting and coordinating regulations was not the only impediment to implementation of the Act. In the months preceding the effective dates of the various regulations, suits were filed against regulatory agencies to enjoin the implementation of the GLBA and the regulations derived therefrom. The Act and regulations were challenged on several grounds, including their constitutionality. In June of 2000, three cases were filed in the Circuit Court for the District of Columbia: Reed Elsevier, Inc. v. Board of Governor,\textsuperscript{63} followed by Trans Union LLC v. Federal Trade Commission,\textsuperscript{64} and finally, Individual Reference Services Group, Inc. v. Federal Trade Commission,\textsuperscript{65} all filed in the Circuit Court of the District of Columbia. Ultimately, the actions were consolidated with one another and with related petitions for review filed against other federal agencies, all challenging the same rules. In the consolidated action, referred to collectively as the Trans Union suit, the Court of Appeals for the District of Columbia held that a financial institution's dissemination of confidential consumer information "warrants reduced constitutional protection." In light of that standard, the privacy regulations created to implement the GLBA were tailored narrowly enough to directly ad-

\textsuperscript{59} 16 C.F.R. § 313.18(b)(1) (2000).


\textsuperscript{63} Reed Elsevier, Inc. v. Bd. of Governors, No. 00-1289 (D.D.C. filed June 30, 2000).

\textsuperscript{64} Trans Union LLC v. FTC, 295 F.3d 42 (D.C. Cir. 2001).

vance the substantial governmental interest in protecting consumer privacy and were therefore constitutional.66

III. ENFORCEMENT OF THE GLBA

The passionate debates over the protection of consumers from the unauthorized disclosure of their confidential financial information have long ago faded from memory. Regulations were drafted. Procedures and standards were created. Notices were sent. Consumers, to the extent they understood the notices at all,67 elected to either "opt-in" or to "opt-out." Yet in the end, individual consumers have not yet realized any significant increase in protection from the handling, or mishandling, of their confidential financial information as a result of the GLBA.

Federal and state regulatory agencies have discovered the enforcement of the Act to be an even greater challenge than the original implementation. The Federal Trade Commission itself was already charged with enforcement of several consumer protection programs, including the Fair Credit Reporting Act68 and the Children's Online Privacy Protection Act.69 Given the FTC's considerable pre-existing enforcement responsibilities and limited resources, unauthorized disclosures of confidential information in violation of the GLBA have not always received the scrutiny they might have warranted. And when FTC enforcement efforts did occur, agencies have often been limited to injunctive relief, with limited recovery of damages to consumers.70

A. GOVERNMENTAL ENFORCEMENT

But for the Trans Union cases filed to enjoin the implementation of the GLBA, many federal functional regulators have not been a party in any action pertaining to the GLBA, including the filing of their own enforcement actions.71 Other regulators, while not filing

66. Trans Union, 295 F.3d at 53.
any actions for the specific purpose of enforcement, have included GLBA compliance as a boiler plate requirement in all stipulated cease and desist orders.\textsuperscript{72}

The FTC has, to date, invested the most effort and resources to enforcement of the Gramm-Leach-Bliley Act. To some degree, the FTC's pre-existing enforcement responsibilities overlapped with those imposed upon it by the GLBA, making enforcement efforts less burdensome. But, given the breadth of its jurisdiction, its enforcement efforts have proceeded only on an industry-by-industry basis or in response to complaints about a particular practice that appears to threaten a large number of consumers.

The FTC's first enforcement initiative was a 2001 investigation labeled Operation Detect Pretext. The FTC reviewed more than 1,000 websites and identified 200 companies (known as information brokers) that offered to obtain and sell consumer asset or bank account information. These information brokers used pretexts to learn a variety of personal information about consumers and then resell that information, violating several laws in the process, including the GLBA, the Federal Credit Reporting Act ("FCRA"), the Drivers Privacy Protection Act ("DPPA"), and the Unfair and Deceptive Trade Practices Act.\textsuperscript{73} The FTC first issued cease and desist letters to the 200 information brokers and issued a consumer alert to the public that was entitled "Pretexting: Your Personal Information Revealed."\textsuperscript{74} Not receiving what it believed to be an appropriate response from these information brokers, the FTC filed its first three enforcement suits on April 18, 2001.\textsuperscript{75}

\textsuperscript{72} See, e.g., In re First Am. Bank, Jackson, MI, Docket No. FDIC-02-032b; In re Family Bank and Trust Co., Palos Hills, IL, FDIC-02-092b; In re Elderton State Bank of Elderton, PA, Docket No. FDIC-03-131b; In re Centennial Bank, Ogden, UT, Docket No. FDIC-03-163b; In re Am. State Bank of Tulsa, OK, Docket No. FDIC-04-245b; In re Cleveland Commercial Bank, S.S.B., Cleveland, Mississippi, F.D.I.C.-04-260b.


\textsuperscript{75} Id.
The three suits, FTC v. Guzzetta, filed in the United States District Court for the District of Maryland,76 FTC v. Information Search, Inc., in the Eastern District of New York,77 and FTC v. Garrett, in the Southern District of Texas,78 alleged that the various defendants used false pretenses (or "pretexts"), fraudulent statements, or impersonation to illegally obtain consumers' confidential financial information. The information brokers would then take their ill-gotten information and sell it on websites for fees ranging from $100 to $600. In sting operations set up by the FTC, investigators posed as purchasers of confidential information. In bringing these suits, the FTC sought to not only warn the information brokers, but to alert the buyers that knowingly obtaining information by pretext is illegal as well.79

Generally, the remedies available to regulatory authorities for violations of the GLBA are somewhat limited, usually injunctive relief and possible "consumer redress or disgorgement."80 One exception is the GLBA's Pretexting procedures. The Pretexting procedures provide for criminal penalties and such actions may be referred to the U.S. Department of Justice.81 Under the GLBA, Subtitle II, it is a federal crime, generally punishable by up to five (5) years in prison, for anyone to use fraud or deception to obtain nonpublic personal information from a financial institution.82 Following the investigation in Operation Detect Pretext, criminal remedies were utilized, giving the FTC greater authority in its enforcement efforts.

One of those actions involved a scam known by the term "phishing." In FTC v. Zachary Keith Hill, the defendant was accused of posing as America Online and e-mailing messages to consumers claiming that there was a problem with their AOL billing.83 The e-mails directed the consumers to immediately update their billing information or risk losing their accounts. The consumers clicked onto a hyperlink in the e-mail and were routed to a site that was virtually identical to

76. FTC v. Guzzetta, Civil Action No. CV 01 2335 (E.D.N.Y. 2001).
82. Id.
AOL's site. The fraudulent site used AOL's logo, AOL's colors, and links to the real AOL site. At the fraudulent site, consumers were induced to provide personal identifying information. The defendants also ran similar phishing scams using Paypal. The FTC's enforcement action resulted in a stipulated preliminary injunction, which was entered on December 17, 2003. But in connection with the efforts of the FTC, the Federal Bureau of Investigation and the United States Attorney for the Eastern District of Virginia investigated and brought criminal charges in the Eastern District of Virginia, Alexandria Division. The Department of Justice ultimately obtained a criminal conviction and Zachary Keith Hill was sentenced to forty-six months in jail.

A second case of phishing was uncovered using the same AOL and Paypal scheme at relatively the same time in California. In FTC v. C.J., the FTC entered into a stipulated permanent injunction with an unnamed minor defendant on July 25, 2003. The minor was prohibited from future violations of the GLBA, from future violations of the FTC Act, and from sending spam. Fines were suspended against the defendant, to be reinstated if the defendant's financial status was proven to be other than as represented. No criminal charges were pursued.

Over the past five years, pretexting violations have been discovered as a result of several FTC investigations. Credit card scams were the basis of enforcement actions in FTC v. Sloniker, FTC v. Assail, Inc., FTC v. Infinium, FTC v. Sun Spectrum Communications Organization, Inc., and FTC v. Sainz Enterprises, LLC. In using the pretext of marketing credit cards, or advance-fee credit cards, defendants often fraudulently obtained personal information from consumers and re-sold the information. In each case, the credit cards were

84. Id.
87. C.J., Civ. No. 03-5275.
specifically marketed to consumers with poor credit histories. Consumers were told that they were entitled to an unsecured major credit card with a significant credit limit for a one-time advance processing fee of usually $150 to $300. Consumers were then asked for financial information such as bank accounts, date of birth, social security number, and personal identifying information, which were to be used for credit purposes. Often, no cards were ever received and if received, they were stored value cards, which had to be loaded with money in advance of use. By the time the scam was detected, the personal information that the consumer had provided was often resold.93

A second scam also directed toward consumers with financial difficulties resulted in a series of enforcement actions filed against debt service operations or credit-counseling services. In 2003, the FTC filed suit against AmeriDebt.94 The FTC alleged that while AmeriDebt advertised itself to be a non-profit credit-counseling service, it was in instead operated to make money for an affiliated entity. The affiliated entity was in essence a finance company. AmeriDebt also took an upfront fee, in contradiction to their advertised statements. In addition to the allegations of fraud, AmeriDebt was accused of violating the GLBA by not providing its customers with required notices advising them how their personal financial information was being used.95

The FTC continued its pursuit of fraudulent practices in the credit-counseling sector in 2004. Between May and November of 2004, three enforcement actions were filed against credit-counseling services, FTC v. National Consumer Council,96 FTC v. Debt Management Foundation Services,97 and FTC v. Better Budget Financial Services.98 In each, a credit-counseling company fraudulently represented itself to be a not-for-profit service, operated to assist consumers in relieving their financial troubles. In fact, the credit-counseling company was a front for pulling in customers, who were then referred to several interrelated companies. These related companies charged upfront fees, and in many instances, customers' debt and in-

95. Id.
terest actually increased. Final settlement of these three actions resulted in more than a combined $6 million in redress to consumers. Settlements also enjoined further violations and implemented monitoring procedures so that the FTC could ensure future compliance.

Violations of the pretexting provisions have proven to be the most frequent type of action pursued. But when the FTC finalized its GLBA Safeguards Rule in 2002, establishing standards and procedures to maintain the security of consumers' financial information, it also created the Safeguards Rule. In industrywide audits of both mortgage companies and automobile dealers, the FTC analyzed compliance with the safety requirements of the rule. In 2004, the FTC filed one of its first cases brought to enforce the Safeguards Rule, In re Sunbelt Lending Services, Inc. In Sunbelt, the defendant was charged with failing to assess risks and implement safeguards to protect confidential customer information, failing to oversee its service providers and loan companies, and failing to provide online consumers with privacy notices.

The second suit brought by the FTC to enforce its Safeguards Rule was In re Nationwide Mortgage Group, Inc. and John Eubank. The charges against Nationwide were similar to those alleged against Sunbelt, but allegedly Nationwide failed to provide privacy notices to customers. Nationwide also failed to train its employees on information security issues, to oversee loan officers in the handling of customer information, and to monitor its computer network.

Finally, in In re Superior Mortgage Corp., the FTC alleged that the defendant violated federal law by failing to provide reasonable security for protected consumer information and for falsely claiming that it encrypted online data. It was ultimately proven that the submitted information was encrypted while it was being transmitted to Superior's website server, but it was decrypted when that information was being forwarded to Superior's main headquarters. Such decryption violated the Safeguards Rule for the protection of consumer information.

102. Id.
104. Id.
106. Id.
One commonality in suits alleging violations of the Safeguards Rule is that the ultimate resolution often involves the implementation of monitoring procedures to insure future compliance. The Sunbelt Lending Services, Inc. case ultimately resulted in a consent agreement being entered into between Sunbelt and the FTC in November of 2004. The consent agreement enjoined Sunbelt from violating the Safeguards Rule and required that Sunbelt's information security program be certified by an expert, chosen by the FTC, annually for ten (10) years.\textsuperscript{107} Nationwide's settlement was similar to that of Sunbelt, but required the evaluations and certifications biennially for ten years.\textsuperscript{108} Superior Mortgage Corp. ultimately agreed to hire an independent third-party auditor to assess its security procedures every two years for the next ten years and to certify that these procedures meet or exceed the protections required by the Safeguards Rule. Superior's settlement also includes record keeping requirements, which allow the FTC to monitor compliance.\textsuperscript{109}

Suits against the mortgage company industry were not limited to violations of the Safeguards Rule. The FTC alleged both pretexting violations as well as safeguards violations in FTC v. 30 Minute Mortgage, Inc., Gregory P. Roth and Peter W. Stolz.\textsuperscript{110} This suit, filed against two individuals and a mortgage company, alleged that the defendants obtained consumer financial information in connection with the deceptive marketing of mortgages.\textsuperscript{111} Although the corporate defendant defaulted, stipulated orders were negotiated with the two individual defendants, which prohibit them from violating the GLBA, the Financial Privacy Rule, the Pretexting provisions, and the Truth in Lending Act or its implementing Regulation Z. The defendants agreed to not make any further misrepresentations related to residential mortgages or to use or benefit from the personal information that they deceptively obtained from consumers. The order required the defendants to post a $1 million bond before sending any future spam.\textsuperscript{112}

Industrywide investigations are the FTC's primary means to enforce the GLBA. Beyond that effort, certain individual scams have

\textsuperscript{107} In re Sunbelt Lending Servs., Inc., FTC File No. 042-3153.
\textsuperscript{108} In re Nationwide Mortgage Group, Inc., FTC File No. 042-3104; FTC Docket No. 9319.
\textsuperscript{109} In re Superior Mortgage Corp., FTC File No. 052-23136.
\textsuperscript{111} 30 Minute Mortgage, Inc., Civ. No. 03-60021.
been so egregious or widespread as to warrant an enforcement action. By way of example, in 2003, suit was filed against National Research Center for College and University Admissions, Inc., American Student List, LLC, and Don M. Munce alleging that the defendants obtained extensive personal information from millions of high school students on the pretext that the information would be provided only to colleges and universities. In fact, the companies also sold students' detailed data to direct marketers, list brokers, and other commercial companies. 113

In November of 2004, the FTC filed suit against a Canadian enterprise for pretexting violations in *FTC v. XTEL Marketing, Inc.* 114 The defendants targeted the elderly, cold calling them and posing as Social Security representatives. The defendants advised the elderly consumer that certain Social Security computer systems had suffered a failure and to ensure receipt of their Social Security benefit payment, the bank account information must be re-entered. Alternatively, these same defendants contacted elderly consumers posing as Medicare representatives and offering a new Medicare insurance program that provided discounts on medication and eyeglasses. The consumer was asked to provide bank account information to allow Medicare to debit the enrollment fee of $299. It was estimated that consumers lost approximately $1 million in these scams. 115

B. Private Enforcement

As discussed, federal and state regulatory agencies' limited resources require that they focus their enforcement investigations on industries or on particular widespread scams. That result may be appropriate because the resulting damages incurred by any consumer are often inconsequential or speculative enough to make the filing of an individual suit impractical. Where does that leave the individual consumers who do not fall within the scope of one of these investigations, whose "rights" under the GLBA have been violated, and who seeks justice? The short answer is, not much better off than they were before 1999.

Emboldened by the protections allegedly granted with the passage of the Gramm-Leach-Bliley Act, consumers whose confidential financial information had been mishandled filed suits to offensively enforce their rights. The threshold issue faced by courts was whether a private right of action existed under the GLBA. While not expressly

115. *Id.* at 5.
addressing the issue of the existence or non-existence of a private right of action, Congress had noted, "This subchapter and the regulations prescribed thereunder shall be enforced by the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to the financial institutions and other persons subject to their jurisdiction." One by one, the courts addressing the issue relied upon this provision to determine that the GLBA did not allow for a private right of action, with little to no additional comment.117

The first two opinions to offer much analysis of the issue were delivered by the United States District Court for the District of Kansas and the Northern District of Illinois. Although both opinions are also unreported, they provide insight into the courts' reasoning in refusing to recognize a private right of action.

In Briggs v. Emporia State Bank and Trust Co.,120 plaintiffs alleged that defendant bank had permitted a bank employee to have access to plaintiffs' banking records and related personal financial statements. The employee allegedly used that information to her own advantage in unrelated litigation between plaintiffs and the employee. The complaint also alleged that the bank was aware of similar conduct by this same employee on other occasions. When the information was utilized as an exhibit during depositions, plaintiffs immediately filed suit against the bank, alleging GLBA violations. The district court, relying upon previous unreported decisions and on the language in 15 U.S.C.A. § 6805, determined that there was no private right of action, express or implied, to consumers under the GLBA.121

In American Family Insurance Company v. Roth,122 American Family filed a non-compete action against a former broker. One claim included in the action was that the broker had taken and used confidential information about insureds, in violation of the rights of those insureds under the Gramm-Leach-Bliley Act. The Roth Court extensively analyzed the availability of a private right of action. Utilizing

121. Id. at *3.
122. Roth, slip op., 2005 WL 3700232.
various rules of statutory construction, the court found it could not reach any other conclusion but that no private right of action existed:

The purpose of the Act was not to create rights but to allow for enhanced competition among entities that hitherto could not compete with each other. The protection of confidential information was ancillary to that goal. More importantly, the existence of a duty imposed by statute on a class of individuals or entities does not perforce create correlative rights in a separate class merely because the latter will receive a benefit from the former's compliance with the imposed duties. For, as the Supreme Court has stressed, "[s]tatutes that focus on the person regulated rather than the individuals protected create 'no implication of an intent to confer rights on a particular class of persons.'" Sandoval, 532 U.S. at 289. Even where a statute was intended to benefit a defined class of individuals, the Supreme Court has held that a private right of action need not necessarily be implied.123

Finding no private right to offensively enforce Gramm-Leach-Bliley violations, individuals next hoped to at least be able to use those rights defensively. The results of the defensive efforts have been mixed. In Marks v. Global Meeting Group, Inc.,124 Union Planters Bank, N.A. v. Gavel,125 and Martino v. Barnett,126 defendant lenders objected to discovery of customer financial information on the grounds that such disclosure would violate the privacy rights of those customers. In each of those actions, the courts relied upon one of several exceptions to the GLBA limitations, including the exceptions for judicial process or fraud.127 On the other hand, in Chao v. Community Trust Co.,128 a Pennsylvania federal court held that it would not compel a party to produce records if to do so would violate an individual's privacy rights under the GLBA.129

In only one case to date has a court held there to be a right to enjoin the disclosure of confidential information protected by the GLBA. In Union Planters Bank, N.A. v. Gavel,130 the plaintiff bank sought an injunction in a state court action to prevent being required to release private consumer financial information. The district court

123. Id. at *8.
granted a permanent injunction under the GLBA.\textsuperscript{131} On appeal, the Fifth Circuit vacated the injunction on other grounds and remanded the case to the district court.\textsuperscript{132} While the Fifth Circuit made no reference in its opinion to the GLBA, it specifically vacated the district court’s opinion on the bank’s GLBA action as well.\textsuperscript{133}

Finally, individual consumers have plead the GLBA as an industry standard creating a duty to the consumer for purposes of negligence or negligence per se. The theory was plead, but not resolved, in \textit{Guin v. Brazos Higher Education Service Corporation, Inc.}\textsuperscript{134} and \textit{Dunmire v. Morgan Stanley DW, Inc.}\textsuperscript{135} In \textit{Guin}, for purposes of summary judgment, the parties conceded that the GLBA established a duty of care.\textsuperscript{136} The court was therefore never afforded the opportunity to consider whether such a duty of care exists. And while the issue may be currently pending in other actions, no opinions have as yet been issued. In \textit{Dunmire}, for purposes of argument on summary judgment, the court assumed that the GLBA established a duty, but held the Act had not been violated.\textsuperscript{137} The fundamental issue of whether the GLBA establishes a duty of care has still not been directly addressed.

CONCLUSION

Five years after its implementation, what has the GLBA accomplished? Has it accomplished its primary purpose of facilitating the sharing of financial data between affiliated entities, so as to allow financial institutions to better compete and thereby reduce costs to consumers? Have its safeguards protected consumers from unauthorized disclosures of confidential financial information? The answers are mixed and the conclusions not final. The GLBA has proven to be a work in progress, which continues to be adjusted as it plays itself out.\textsuperscript{138} In the short term, most consumers are not likely to see its effects beyond yearly written notices, and most financial institutions are not likely to see its effects beyond increased procedures and

\begin{itemize}
\item \textsuperscript{131} \textit{Union Planters Bank}, 2003 WL 1193671, at *5-*9.
\item \textsuperscript{132} \textit{Union Planters Bank Nat'l Ass'n v. Salih}, 369 F.3d 457 (5th Cir. 2004).
\item \textsuperscript{133} \textit{Salih}, 369 F.3d at 463 n.10.
\item \textsuperscript{134} \textit{2006 WL 288483} (D.Minn. Feb. 7, 2006).
\item \textsuperscript{135} \textit{2005 U.S. Dist. LEXIS 33496}, Case No. 4:04-CV-01059 (W.D. Mo. Apr. 7, 2005).
\item \textsuperscript{137} \textit{Dunmire v. Morgan Stanley DW, Inc.}, 2005 U.S. Dist. LEXIS 33496, Case No. 4:04-CV-01059 (W.D. Mo. Apr. 7, 2005).
\end{itemize}
paperwork. But while not immediate, the GLBA will hopefully prove to be the start of a change in attitude; a change that acknowledges and protects individuals' privacy rights, even in the face of commercial progress. The GLBA has proven not to be a destination, but the beginning of a journey.