I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

SARAH ELIZABETH EXTEN*

Major Developments in Financial Privacy Law 2006: The SWIFT Database Incident, and Updates to the Gramm-Leach-Bliley and Fair Credit Reporting Acts

Abstract: As technological developments create new ways to access information, it becomes even more important that users know that the entities responsible for protecting their personal data are actually doing so. A significant development in this regard was the revelation that SWIFT supplies the U.S. government with users' financial transaction information. Additionally, since the inception of the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, financial privacy law developments have come in the form of a Supreme Court decision and an interagency action to change notice forms.

* The author is a Juris Doctor candidate at The Ohio State University Moritz College of Law, class of 2008. She graduated *magna cum laude with Honors* from The Ohio State University with a major in English and a minor in Italian.

I. INTRODUCTION

The realm of financial privacy experienced many significant developments this year. The most publicized of those was the revelation of the United States' use of the SWIFT database to monitor terrorists' activities via financial transfers. Within days after the story broke, experts in the United States called into question the validity of this practice and whether or not it violated U.S. law. EU leaders also expressed concern, stating that even if no U.S. laws were violated, there still may be a problem under EU law. Throughout the controversy, though, both the U.S. government and SWIFT have maintained the validity of the program in all affected countries.

The Grahm-Leach-Bliley Act ("GLBA") also experienced some intriguing developments this year. First, legislation was enacted that affects the application of the GLBA to certified public accountants ("CPA"). Second, the Mississippi Supreme Court addressed the GLBA's application to trial discovery of financial information. Third, whether banks will be covered under the GLBA in the future has been questioned due to proposed regulatory schemes on that issue.

Finally, the Fair Credit Reporting Act ("FCRA") has also been the subject of some significant developments this year. The most notable development came by way of a U.S. Supreme Court decision that focused on specific sections of the FCRA in relation to the requirements for showing an adverse action under the Act. Three lower court decisions also addressed application of the FCRA. One of these attempted to clarify the definition of legitimate business need, while the other two helped illuminate what exactly constitutes a firm offer of credit, "clear and conspicuous" notice to a customer, and what constitutes a willful violation of the Act.

All of these developments, though they may be separate and unique from one another, are of great significance to the world of financial privacy. Each development brings with it the possibility, if not the promise, of significant changes to how financial privacy is approached. As such, it is vital that they all be monitored in the coming months and years to see what the future developments will be.

II. THE SWIFT DATABASE AS A TERRORIST TRACKING TOOL

A. INTRODUCTION

On June 23, 2006, The New York Times published a story on a post-September 11 anti-terrorism program that utilized the personal

banking data of thousands of Americans and foreigners by way of the SWIFT Database.[1] The reaction to this information was rapid. The U.S. government insisted that everything it did was perfectly legal and berated The New York Times and other media outlets for reporting the story.[2] Even assuming the government proves the facial legality of the program, the use of the SWIFT database is still problematic, as "[t]here is a high risk that innocent citizens' sensitive financial data was scrutinized under this program"[3] and the Treasury Department alone monitors the use of the data, with "no outside governmental official, such as a federal judge, review[ing] the program."[4] The European Union voiced serious concerns as to whether or not the SWIFT Company was violating any EU laws by releasing the data.[5] The answers to the questions raised by the use of the SWIFT database have been the focus of much of the privacy world in recent months, and is the initial focus of this paper as well.

B. THE DATABASE

The Society for Worldwide Interbank Financial Telecommunications ("SWIFT") is a third-party messaging service and software company that handles international money transfers for approximately 8,000 financial institutions, spanning 206 countries and territories.[6] The company is incorporated under Belgian law and is

---

[1] Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A10; James Risen, *US Reaches Tentative Deal with Europe on Bank Data*, N.Y. TIMES, June 29, 2007, at A6.

[2] Sheryl Gay Stolberg & Eric Lichtblau, *Cheney Assails Press on Report on Bank Data*, N.Y. TIMES, June 23, 2006, at A1.

[3] *Spotlight on Surveillance June 2006: Treasury's International Finance Tracking Program of Questionable Legality*, ELEC. PRIVACY INFO. CTR., http://www.epic.org/privacy/surveillance/spotlight/0606/ (last visited Jan. 29, 2008).

[4] *Id.*

[5] *Europe's Privacy Commissioners Rule against SWIFT,* PRIVACY INT'L, Nov. 24, 2006, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-546365.

[6] SWIFT.com, *About SWIFT–Company Information*, http://www.swift.com/index.cfm?item_id=41322 (last visited Jan. 29, 2008). SWIFT.com, *SWIFT in Figures*, http://www.swift.com/index.cfm?item_id=64389 (last visited Jan. 29, 2008). The SWIFT database is "the industry-owned co-operative supplying secure, standardized messaging services and interface software to nearly 8,000 financial institutions in 206 countries and territories. SWIFT members include banks, broker-dealers and investment managers. The broader SWIFT community also encompasses corporate as well as market

governed by a committee of 25 independent directors elected by its shareholders.[7] SWIFT "routes about $6 trillion daily between banks, brokerages, stock exchanges and other institutions. The records mostly involve wire transfers and other methods of moving money overseas and into and out of the United States. Most routine financial transactions confined to this country are not in the database."[8] Due to the highly sensitive and private nature of the information being transferred, the SWIFT database is overseen by the central banks of the Group of Ten countries ("G-10").[9] This practice was initiated in 1998 and underwent changes in 2004 to strengthen the power of the G-10.[10] Because SWIFT is incorporated in Belgium, the National Bank of Belgium ("NBB") is the G-10 bank most involved in the oversight activities.[11] The NBB carries out its duties by monitoring a variety of official documents created by SWIFT, including reports on security audits, incidents, and incident review, as well as papers generated by the board.[12] SWIFT aids the NBB in this process by identifying additional materials that may be relevant.[13] This information is then

---

infrastructures in payments, securities, treasury and trade." SWIFT.com, *SWIFTNet Trade Services Utility*, http://www.swift.com/index.cfm?item_id=60657 (last visited Jan. 29, 2008).

[7] SWIFT.com, *Governance at SWIFT*, http://www.swift.com/index.cfm?item_id=1241 (last visited Jan. 29, 2008).

[8] Lichtblau & Risen, *supra* note 1.

[9] SWIFT.com, Governance–Oversight of SWIFT, http://www.swift.com/index.cfm?item_id= 57001 (last visited Jan. 29, 2008). The G-10 refers to "the group of countries that have agreed to participate in the General Arrangements to Borrow (GAB), a supplementary borrowing arrangement that can be invoked if the IMF's resources are estimated to be below member's needs. The GAB was established in 1962, when the governments of eight IMF members—Belgium, Canada, France, Italy, Japan, the Netherlands, the United Kingdom, and the United States—and the central banks of two others, Germany and Sweden, agreed to make resources available to the IMF for drawings by participants, and, under certain circumstances, for drawings by nonparticipants. The GAB was strengthened in 1964 by the association of Switzerland, then a nonmember of the Fund, but the name of the G-10 remained the same. The following international organizations are official observers of the activities of the G-10: The Bank for International Settlements (BIS), European Commission, IMF, and OECD." International Monetary Fund, *Factsheet–A Guide to Committees, Groups and Clubs*, Aug. 2006, http://www.imf.org/external/np/exr/facts/ groups.htm.

[10] SWIFT.com, *supra* note 9.

[11] *Id.*

[12] *Id*.

[13] *Id.*

made available to the other G-10 countries, which rely on the NBB to be their eyes and ears with regards to the monitoring activities.[14]

C. THE U.S. GOVERNMENT'S USE OF SWIFT

Although the world did not learn of the U.S. government's use of the SWIFT database until The New York Times leaked the story, this controversial partnership began shortly after the terrorist attacks of September 11.[15] The government believed that tracking international monetary transfers could provide crucial information regarding the whereabouts of key al Qaeda members, as well as others who pose a threat to U.S. security.[16]

In order to gain access to the information, the government established a program run by the CIA and overseen by the Treasury Department.[17] The Treasury Department made use of a broad administrative subpoena, as opposed to numerous individual ones, in order to gain access to millions of records in the SWIFT database.[18] An administrative subpoena is "an order from a government official to a third party, instructing the recipient to produce certain information. Because the subpoena is issued directly by an agency official, it can be issued as quickly as the development of an investigation requires."[19]

---

[14] *Id.*

[15] Lichtblau & Risen, *supra* note 1.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists: Hearing Before the Subcomm. on Terrorism, Tech. and Homeland Sec. of the S. Judiciary Comm., 109th Cong. (2004) (testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice), *available at* http://kyl.senate.gov/legis_center/subdocs/062204_brand.pdf. The Republican-led Senate Intelligence Committee pushed for changes to the administrative subpoena powers under the USA PATRIOT Act that would have expanded the USA PATRIOT Act to allow the FBI to demand records in terror investigations through administrative subpoenas, without a judge's order, and to have sole discretion in deciding whether to monitor the mail of terror suspects. This part of the USA PATRIOT Act, however, was not passed in order to allow for quick reauthorization of the Act. *See also* Eric Lichtblau, *Senate Makes Permanent Nearly All Provisions of Patriot Act, With a Few Restrictions*, N.Y. TIMES, July 29, 2005, at A11.

The government maintains that using administrative subpoenas in this way violates no currently operational privacy laws.[20] The only law tailored to the issue, the Right to Financial Privacy Act of 1978 ("RFPA"), is limited in scope and includes numerous exceptions.[21] The RFPA was enacted in 1978 in response to the Supreme Court's holding in *United States v. Miller*, 425 U.S. 435 (1976), where it held there was no legitimate expectation of privacy for financial information held by financial institutions.[22] The RFPA "requires that federal government agencies provide individuals with a notice and an opportunity to object before a bank or other specified institution can disclose personal financial information to a federal government agency."[23]

Further, it "provides civil remedies against the government and banks for disclosures of a bank customer's financial information without consent, or a valid warrant or subpoena."[24] However, there are exceptions to general protections of the RFPA. One such exception is found under 12 U.S.C. §3414(a)(1)(A), which states that nothing in that chapter (with some exceptions) will be applied to "the production and disclosure of financial records pursuant to requests from . . . a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities."[25] Under the language of this exception, the executive is fully within the power delegated to it by Congress in issuing and acting upon the administrative subpoena. Further, there is no Fourth Amendment protection for these records. The Supreme Court held in *United States v. Miller* that the Fourth Amendment does not cover financial transaction records held by third parties such as banks, since there is no legitimate expectation of privacy in such records.[26] While the RFPA was created in response to this case

---

[20] Lichtblau & Risen, *supra* note 1.

[21] *See* Right to Financial Privacy Act of 1978, Pub L. No. 95-630; 92 Stat. 3697 (codified at 12 U.S.C. §§ 3401–3422).

[22] *The Right to Financial Privacy Act*, ELEC. PRIVACY INFO. CTR., http://www.epic.org/privacy/rfpa/ (last visited Jan. 29, 2008).

[23] *Id.*

[24] David Ziemer, *No Privacy Interest in Bank Records*, WIS. L.J., Dec. 20, 2006, http://www.wislawjournal.com/archive/2006/1220/bank.html.

[25] 12 U.S.C. § 3414 (2007).

[26] United States v. Miller, 425 U.S. 435, 442 (1976).

specifically, it only provides civil remedies, as opposed to an exclusionary one that would allow information obtained in violation of the Fourth Amendment to be excluded from use in trial.[27]

Aside from the Right to Financial Privacy Act, other statutes and constitutional provisions are implicated. One such provision is the International Emergency Economic Powers Act ("IEEPA") which "gives the President what legal experts say is wide authority to 'investigate, regulate or prohibit' foreign transactions in responding to 'an unusual and extraordinary threat.'"[28] The threat posed by September 11 falls within the language of the IEEPA and therefore, arguably, allows the President access to the SWIFT database under the language of the Act.[29] However, there is no express language in either statute stating that the IEEPA trumps the RFPA.

Because the government asserts that it has been acting fully within the law in pursuing this program, the outcry from Washington against the media's publication of this data has been fierce and swift. Vice President Dick Cheney, at a press conference soon after the leak, chastised the media for disclosing "vital national security programs" and thereby making it more difficult to conduct the programs aimed at protecting the American people.[30] Soon after The New York Times printed the story regarding the government's use of the SWIFT database, it reported an anticipated House Resolution that would bolster the power of the government to track terrorism via financial records, and put more pressure upon the media to avoid publication of government security programs and all the relating details.[31] One member of Congress, Representative Peter T. King (R-NY), went so far as to say that members of The New York Times responsible for the leak ought to be imprisoned for their actions.[32]

---

[27] Ziemer, *supra* note 24.

[28] Anita Ramasastry, *The Treasury Department's Secret Monitoring of International Funds Transfers*, FINDLAW, http://technology.findlaw.com/articles/00006/010162.html (last visited Jan. 29, 2008).

[29] International Emergency Economic Powers Act, Pub. L. No. 110-96 (2007) (codified at 50 U.S.C. §§ 1701–1707).

[30] Stolberg & Lichtblau, *supra* note 2.

[31] *See* H.R. Res. 896, 109th Cong. (2006), *available at* http://www.fas.org/irp/congress/2006_cr/h062906.html.

[32] Scott Shane, *Behind Bush's Fury, a Vow Made in 2001*, N.Y. TIMES, June 29, 2006, at A4.

The Director of National Intelligence, John D. Negroponte, further responded to The New York Times' leak of the information by launching an investigation into whether providing this information to the public has damaged the nation's counter-terrorism efforts in any way.[33] However, whether there will actually be any appreciable impact on the effectiveness of the government's program is debatable, as opined by experts on the subject of terrorist financing.[34] On one hand, some feel that the terrorists likely knew about the government's program before the leak and that the only persons truly caught off-guard by the media's revelation were the bankers.[35] If this is the case, though, there is still some possible harm, as bankers and other financial institutions may become more resistant to sharing their records with the government if they know what the possible use for the information may be.[36] On the other hand, some feel that the terrorists had no inkling of the existence of the government's program and will respond by avoiding the banking system as a means to move money.[37]

Under this scenario, there are two views espoused. Some feel that having the terrorists pull out of the banking system will be very harmful to the ability of the United States and its allies to monitor the activities of terrorists, due to the banking system's effectiveness as a tracking tool.[38] Alternatively, some feel that nothing will change, since they claim that terrorists likely already knew of this monitoring prior to the publication of The New York Times article.[39]

---

[33] *Id.*

[34] *Id.*

[35] *Id*.

[36] *Id*.

[37] *Id.*

[38] *Id. See also* Scott Shane, *Damage Study Urged on Surveillance Reports*, N.Y. TIMES, June 28, 2006, at A12.

[39] Bryan Bender, *Terrorist Funds-Tracking No Secret, Some Say*, BOSTON GLOBE, June 28, 2006, at A1.

D. REACTION FROM THE EUROPEAN UNION AND RESPONSE FROM SWIFT

While the use of the SWIFT database to track terrorism may not violate any U.S. law, many in the European Union ("EU") have asserted that SWIFT, a Belgian entity,[40] violates EU law, Directive 95/46/EC, by providing the U.S. with information from its database.[41] The Belgium Commission on Privacy Protection found that under Article 29 Section 1 of the Belgian Data Protection Law ("DPL"), regarding the processing of personal data, SWIFT:

> at the least committed a number of errors of judgment when dealing with the American subpoenas . . . [which] must be considered a serious error of judgment on the part of SWIFT to subject a massive quantity of personal data to surveillance in a secret and systematic manner for years without effective grounds for justification and without independent control in accordance with Belgian and European law."[42]

The language of Directive 95/46/EC states that, in general, the personal privacy of the individual and the individual's ability to control the free flow of his or her personal information is paramount to the interest of banks and third parties in accessing their information.[43] Further, it is the duty of EU member states to protect these rights.[44] Under this Directive, there must be a lawful basis for accessing personal data. Reasons listed in the Directive that allow data to be processed for release to third parties include: (1) it is in the public interest to process the data based on manifested treaties; (2) the institution or third party requesting the data has the official authority to

---

[40] *Belgium Privacy Commission Reviews SWIFT Violation of Data Protection Law*, BESPACIFIC, Oct. 2, 2006, http://www.bespacific.com/mt/archives/012672.html.

[41] Council Directive 95/46, 1995 O.J. (L 281) (EC), *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; Doug Cameron & Sarah Laitner, *Fresh Drive to Tackle Dispute on Data from Passengers*, FIN. TIMES, Oct. 5, 2006, at 6.

[42] *Belgium Privacy Commission Reviews SWIFT Violation of Data Protection Law*, *supra* note 40.

[43] *See* Council Directive 95/46, *supra* note 41.

[44] Council Regulation 45/2001, 2001 O.J. (L 8) 1 (EC), *available at* http://europa.eu/eur-lex/pri/en/oj/dat/2001/l_008/l_00820010112en00010022.pdf.

do so; (3) the institution processing the data bears a legal obligation to do so; (4) the data subject has given his or her consent; (5) the data subject is entering into a contract that mandates the release of the data; or (6) it is necessary to process the data to protect the vital interests of the subject.[45] On the basis of the Directive, Belgium has declared that SWIFT's actions are illegal, finding it to be a data controller, not a processor, and therefore subject to a higher privacy standard.[46]

One of the main problems identified by EU privacy campaigners is that regardless of the U.S. government's guarantees regarding its handling of data, neither SWIFT nor the European regulators will have the ability to control how the data is used once the data has been released.[47] The EU contends that SWIFT is subject to the Directive, even though SWIFT is not a bank or other form of financial institution, because it is a "controller" of personal data under the language of the Directive and therefore must comply with the Directive's rules.[48] Under the Directive:

> 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; and 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.[49]

---

[45] *Id*. at 5–6.

[46] Article 29 Data Protection Working Party, *Opinion 10/2006: On the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, 01935/06/EN WP128 (Nov. 22, 2006), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf.

[47] Michael Peel, *Call to Resolve US and EU Privacy Conflict*, FIN. TIMES, Nov. 17, 2006, http://search.ft.com/ftArticle?queryText=Call+to+Resolve+US+and+EU+Privacy+Conflict&y=6&aje=true&x=8&id=061117001041&ct=0.

[48] Article 29 Data Protection Working Party, *supra* note 46.

[49] Council Directive 95/46, ch. I, art. 2(d), (e).

SWIFT counters the argument that it is a controller by asserting that, regardless of the nature of the data that it handles, the company is little more than a processor of that data and therefore it is not subject to the same rules and regulations as the institutions whose data it handles.[50] This controller/processor distinction is critical because if SWIFT is in fact the controller of the data, as opposed to a mere processor, then it would be subject to a higher privacy standard and would have more obligations under the Directive than processors, who merely do what those whom they work for tell them to do, and, therefore, be more accountable for its divulging of the data to the U.S.[51] In addition, the German government has begun to voice concerns that potential violations of EU law might not only hurt bank customers, but may also work against the U.S. government's goal of battling terrorism.[52]

If it turns out that laws were violated in the execution of the subpoena, tensions between the U.S. and EU member states concerning the war on terror and the privacy of EU citizens may be seriously aggravated.[53] Both the U.S. and SWIFT respond to the allegations of illegality by maintaining that the data releases are legitimate.[54] SWIFT also argues that, regardless of whether it is considered a data controller or a data processor under the language of Directive 95/46/EC, there are serious interpretation issues regarding the current data privacy law.[55] According to SWIFT, Directive 95/46/EC was created in an era when the authorities focused little

---

[50] SWIFT Statement on Compliance to European Parliament, Oct. 4, 2006, *available at* http://www.swift.com/index.cfm?item_id=60670.

[51] Council Directive 95/46, ch. I, art. 2(d), (e); "Opinion delivered by ICPP on August 23rd, 2006: International wire transfer by Schleswig-Holstein banks using SWIFT," Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/wirtschaft/swift/060825_swift_en.htm (last visited Jan. 29, 2008).

[52] Mark Schieritz, Ralph Atkins & Birgit Marshall, *German Concern over Transfer of Bank Data to US.*, FIN. TIMES, Sept. 6, 2006, available at http://search.ft.com/ftArticle?queryText=German+Concern+at+Swift+Disclosure&y=6&aje=false&x=9&id=060906000768&ct=0.

[53] *Id.*

[54] *Id.*; Stolberg & Lichtblau, *supra* note 2.

[55] Compare the language of the Directive in 1995 to SWIFT's response. *See* Council Directive 95/46, ch. II; SWIFT.com, *US Terrorist Financing Investigations and the Role of SWIFT*, Feb. 11, 2007, http://www.swift.com/index.cfm?item_id=61228#section2.

attention on the financial activities of terrorist organizations. But the world has changed since 1995, and since September 11, many feel that monitoring terrorists' finances has become a crucial tool in the War on Terror.[56] SWIFT asserts that they have followed all applicable laws and are doing nothing illegal, in fact they claim they are helping to affect one of the United States' most important national security goals—tracking the movement of terrorists by monitoring their bank accounts.[57]

Along with arguing that EU law is outdated, SWIFT also stresses the fact that it has taken the utmost care to protect the privacy of the people whose data is released to the U.S. government under the administrative subpoena.[58] First and foremost, SWIFT maintains that the data searches performed by the U.S. were both controlled and audited under the supervision of the U.S. Treasury Department, which headed the searches and was in full compliance with U.S. law.[59] This argument is not readily accepted by the international community; Germany, for example, maintains that legality in the eyes of U.S. law does not determine if these searches violated German law. Also, SWIFT identified that it has carried out similar subpoenas within the U.S., as much of SWIFT is based within the United States. Finally, SWIFT has defended its actions by stressing that it places a great deal of importance upon the idea of data confidentiality.[60]

E. CONCLUSION

Even though the United States government's use of the SWIFT database was made known to the world in the summer of 2006, the true repercussions of its revelation are yet to be seen. As of this writing, the European Union has yet to decide definitively if the SWIFT database is covered under the EU Directive, which it must do before it can address the more important question of whether or not the company actually violated any part of it. Nevertheless, EU lawmakers have voiced anger at the agreement between SWIFT and the U.S. to

---

[56] Shane, *supra* note 32, at A4.

[57] Swift.com, *supra* note 55.

[58] *Id.*

[59] *Id.*

[60] Council Directive 95/46, at 41.

transfer secret banking information.[61] The ultimate repercussion for the media is also unknown. How far will the government go to control the flow of information to the public? Will the U.S. government undermine the First Amendment rights of the press in the name of protecting national security? More importantly, will leaking the existence of the program hurt the war on terror? Some of these questions may be answered as the situation develops over the coming months.[62]

III. UPDATES TO THE GRAMM-LEACH-BLILEY ACT

A. INTRODUCTION

In the past year, there have been some significant changes to the Gramm-Leach-Bliley Financial Services Modernization Act.[63] First, legislation was enacted that affects the application of the GLBA to certified public accountants. Second, a recent Mississippi Supreme Court decision addresses the application of the GLBA to trial discovery. Finally, regulatory schemes were proposed that may affect coverage of banks under the GLBA. While these developments are small in number, their impact may be large, and they certainly suggest that the GLBA may experience some changes in the near future.

B. SECTION 609 OF THE FINANCIAL REGULATORY RELIEF BILL

When the GLBA was first passed, it required certified public accountants to send annual privacy disclosure notices to their clients.[64]

---

[61] *U.S. Mines European Bank Data, Angers EU Authorities*, LAW.COM, July 6, 2006, http://www.law.com/jsp/article.jsp?id=1152090320360.

[62] To follow Europe's treatment of SWIFT, *see* Article 29 Data Protection Working Party, *supra* note 46.

[63] For a review of previous developments concerning GLBA, *see* Richard Joseph McMahon, Note, *Developments in the Gramm-Leach-Bliley Act During 2005-06: An Overview of Important Changes in Case Law and Pending Legislation*, 2 ISJLP 737 (2006).

[64] *See* Gramm-Leach-Bliley Act, § 503(a), Pub. L. No. 106-102, 113 Stat. 1338, 1439 (1999) (codified at 15 U.S.C. § 6803 (2000 & Supp. V)). "The GLBA primarily sought to 'modernize' financial services–that is, end regulations that prevented the merger of banks, stock brokerage companies, and insurance companies. The removal of these regulations, however, raised significant risks that these new financial institutions would have access to an incredible amount of personal information, with no restrictions upon its use. Prior to GLBA, the insurance company that maintained your health records was distinct from the bank that mortgaged your house and the stockbroker that traded your stocks. Once these companies

Many felt that this requirement was not only unnecessary, but also harmful to the accountants. The president of the American Institute of Certified Public Accountants ("AICPA"), Barry Melancon, claimed that the requirements of the GLBA were redundant as applied to CPAs, that the notices did little more than confuse their clients, and that the notices required substantial time to prepare.[65] Section 609 of the Financial Regulatory Relief Bill (S.B. 2856), which was signed into law by President George W. Bush on October 13, 2006, exempted CPAs from the requirements for disclosure under section 503(a) of GLBA.[66]

C. *CAPITAL ONE SERVICES, INC. V. PAGE*

In *Capital One Services, Inc. v. Page*,[67] the Mississippi Supreme Court addressed the issue of whether a trial court's order to produce information of third-party Capital One customers with accounts similar to the account of respondent Page "would violate provisions in the GLBA that protect the privacy of personal financial information."[68] Page filed suit against Capital One for failure to disclose specific terms of a credit card account that Page opened with the company.[69] Unknown to Page, the account was subject to additional fees and charges that led to Page owing Capital One a large amount of money.[70] During discovery, Page requested a list of all Mississippians to whom

---

merge, however, they would have the ability to consolidate, analyze and sell the personal details of their customers' lives. Because of these risks, the GLBA included three simple requirements to protect the personal data of individuals: First, banks, brokerage companies, and insurance companies must securely store personal financial information. Second, they must advise you of their policies on sharing of personal financial information. Third, they must give consumers the option to opt-out of some sharing of personal financial information." Electronic Privacy Information Center, *The Gramm-Leach-Bliley Act*, http://www.epic.org/privacy/glba/ (last visited Jan. 29, 2008).

[65] *Senate Passes Financial Regulatory Relief; Bill Expected to Earn President's Signature*, 6 PRIVACY L. WATCH (BNA) No. 192 (Oct. 4, 2006).

[66] Financial Services Regulatory Relief Act of 2006, § 609, Pub. L. No. 109-351, 120 Stat. 1966, 1983 (to be codified at 15 U.S.C. § 6803).

[67] Capital One Servs., Inc. v. Page, 942 So. 2d 760 (Miss. 2006).

[68] *Credit Card Firm Told to Produce Data as Court Rejects Defense Based on GLB Act*, 6 PRIVACY L. WATCH (BNA) No. 223 (Nov. 20, 2006).

[69] *Capital One Servs., Inc.*, 942 So. 2d at 761.

[70] *Id.*

Capital One issued similar accounts between January 1, 1999 and April 13, 2004.[71] Capital One objected to Page's requests, but the trial court granted Page's motion to compel, subject to a confidentiality agreement and specific strict limitations regarding how the information could be used.[72] Page subsequently won at trial and Capital One brought the case on appeal before the Mississippi Supreme Court.[73]

The Mississippi Supreme Court held that, "[t]he GLBA does not prohibit the strictly limited disclosure in discovery of the names and addresses of other Mississippians who completed [acceptance certificate forms] identical to that completed by Page. This information is reasonably calculated to lead to admissible evidence."[74] The court observed that while the GLBA provides that "a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title,"[75] there is an exception where disclosure is necessary "to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law."[76]

The court went on to note that it was not alone in this view of the application of the GLBA, because the highest courts in Alabama and West Virginia, as well as the federal district courts in Texas and West Virginia, have adopted a similar exception by allowing discovery of consumer information in civil cases.[77] In the court's opinion, this view is justified because "[t]he legislative history indicates that the House

---

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.* at 765.

[75] *Id.* at 762 (citing 15 U.S.C. § 6802(a)).

[76] *Id.* (citing 15 U.S.C. § 6802(e)(8)).

[77] *Id.*; *see* Choate v. State Farm Lloyds, No. Civ.A. 3:03-CV-2111-M, 2005 WL 1109432, at *4 (N.D. Tex. May 5, 2005); Marks v. Global Mortgage Group, Inc., 218 F.R.D. 492, 496 (S.D. W. Va. 2003); *Ex parte* Nat'l W. Life Ins. Co., 899 So. 2d 218, 226–27 (Ala. 2004); Martino v. Barnett, 595 S.E.2d 65, 72 (W. Va. 2004).

Bill, which added the privacy protections to the GLBA, envisaged an independent judicial process exception," and the disclosure of information by a party pursuant to a court order is considered engaging in a judicial process.[78]

D. PRIVACY NOTICES

Significant developments have also occurred in the area of privacy notices. Seven GLBA agencies—the Federal Trade Commission ("FTC"), the Board of Governors of the Federal Reserve System ("FRB"), the Office of the Comptroller of the Currency ("OCC"), the Federal Deposit Insurance Corporation ("FDIC"), the Securities and Exchange Commission ("SEC"), the National Credit Union Administration ("NCUA"), and the Office of Thrift Supervision ("OTS") in Treasury—are working to develop alternative forms of consumer privacy notices.[79] On March 21, 2007, the Commodity Futures Trading Commission ("CFTC") and the seven GLBA agencies ("the Agencies") proposed a new rule under the GLBA what commentators were encouraged to entitle the "Model Privacy Form" in order to "facilitate the organization and distribution of comments among the Agencies."[80] This proposal requires financial institutions to provide both initial and annual privacy notices to customers.[81] It includes a safe harbor model privacy form, which would be used by institutions when providing disclosures under the privacy rules.[82] The proposed rule is being enacted pursuant to the authority in sections 503

---

[78] *Capital One Servs., Inc*, 942 So. 2d at 763; *see generally* McMahon, *supra* note 63 (further information on the GLBA, including differing interpretations of other courts).

[79] Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act, 72 Fed. Reg. 14,940, 14,940 (Mar. 29, 2007), *available at* http://ftc.gov/os/2007/03/CorrectedNeptuneMarsandGenericFormsfrn.pdf. For additional information, *see* Federal Trade Commission, *Financial Privacy Rule: Interagency Notice Research Project*, http://ftc.gov/privacy/privacyinitiatives/financial_rule_inrp.html (last visited Jan. 29, 2008).

[80] Interagency Proposal for Model Privacy Form under the Gramm-Leach-Bliley Act, *supra* note 79, at 14,940.

[81] *Id.* at 14,943.

[82] *Id.* at 14,940.

and 504 of the GLBA as amended by section 728 of the Financial Services Regulatory Relief Act of 2006.[83]

In August 2004, the FTC, FRB, OCC, FDIC, SEC, and NCUA issued a Statement of Work, which described the research design these six agencies were using in an attempt to create alternative forms of notice for consumers.[84] In it, they noted that the overall objective of this project is to "design alternative privacy notices that are easier for consumers to understand and use, relative to current privacy notices commonly used by financial institutions."[85] The research was conducted by Kleimann Communication Group and was made available for public comment until the end of May 2007.[86] In general, the commentators supported some of the aspects of the proposal; however, they also sought more flexibility in other aspects.[87] Specifically, the major banking institutions felt the forms should be shorter and more flexible.[88] Furthermore, the bankers took issue with an aspect of the proposal that eliminated safe harbor provisions that allowed groups "to use existing privacy notice language for one year if they make more than minor changes to the model language."[89] However, as of this writing, no further developments have been made regarding the model privacy forms.

---

[83] *Id.* at 14,956. For a section-by-section description of the Bill, *see* Independent Community Bankers of America, *Financial Services Regulatory Relief Act of 2006*, http://www.icba.org/files/ICBASites/PDFs/2006regreliefbill.pdf (last visited Jan. 29, 2007).

[84] *Financial Privacy Rule: Interagency Notice Research Project*, *supra* note 79; Federal Trade Commission, *Statement of Work: Form Development Project Designing Easy-to-Understand Consumer Financial Privacy Notices* [hereinafter *FTC Statement of Work*], http://ftc.gov/privacy/glbact/sow_privacy_notice_final1.pdf (last visited Jan. 29, 2008).

[85] *FTC Statement of Work*, *supra* note 84, at 1.

[86] *Financial Privacy Rule: Interagency Notice Research Project*, *supra* note 79. *See generally* U.S. Securities and Exchange Commission, *Comments on Proposed Rule: Interagency Proposal for Model Privacy From Under the Gramm-Leach-Bliley Act*, http://www.sec.gov/comments/s7-09-07/s70907.shtml (last visited Jan. 29, 2008) (listing persons who commented on the form with links to their comments).

[87] Marcia Kass, *Financial Groups Critique Interagency Model Privacy Form Proposal under GLB Act*, 7 PRIVACY L. WATCH (BNA) No. 104 (May 31, 2007).

[88] *Id.*

[89] *Id.*

E. OTHER CONSIDERATIONS

One final issue is whether lawyers are considered to be "service providers" under the provisions of the GLBA.[90] If so qualified, "[l]awyers representing GLBA-regulated financial institutions may be required to give contractual assurances about their information security practices and, in particular, the steps they are taking to protect any personal information they may acquire in the course of their representation."[91] While there is no ruling on point from the Supreme Court, this is an issue that could directly affect the practice of lawyers who represent financial institutions falling under the regulations of the GLBA.[92] Service providers are subject to safeguard rules only, and not privacy rules, as the FTC "already requires financial institutions to oversee their service providers by 'taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue' and 'require service providers by contract to implement and maintain such safeguards.'"[93] Furthermore, the legal profession itself already requires a professional duty of confidentiality.[94] As such, this is an area of particular importance to the legal profession that should be watched carefully in the future as developments in the law under the GLBA occur.

IV. UPDATES TO THE FAIR CREDIT REPORTING ACT

A. INTRODUCTION

The Fair Credit Reporting Act ("FCRA") was enacted in order to "insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality and a respect for the

---

[90] *See* Posting of Peter Mucklestone & Stuart Louie to Privacy and Security Law Blog, http://www.privsecblog.com/archives/financial-institutions-lawyers-as-service-providers-under-the-grammleachbliley-act.html (June 8, 2006).

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

consumer's right to privacy."[95] The Supreme Court recently decided a case interpreting this Act.[96] There have also been developments in the state and federal courts. Two issues were addressed in three cases during the past year: using consumer credit reports to assess a patient's ability to pay for medical services, and directing targeted marketing campaigns at individuals based on information obtained from their consumer credit reports.

B. SUPREME COURT INTERPRETATION OF THE FCRA

In June 2007, the Supreme Court decided *Safeco Insurance Company of America v. Burr*.[97] The issues in this case were whether the "willful failure" language in § 1681n(a) of the FCRA covers violations committed in reckless disregard of the notice obligation, and, if so, whether the initial rate charges for new insurance policies based on consumer credit reports are "adverse actions" requiring notice under the FCRA.[98] In regards to the first issue, the Supreme Court held that the willfulness language under § 1681n(a) of the Act applies to reckless disregard of a statutory duty, not just knowing violations of the Act, as the petitioners argued.[99]

Turning to the second issue, the Court held that "the 'increase' [in the rate] required for 'adverse action,' 15 U.S.C. § 1681a(k)(1)(B)(i), speaks to a disadvantageous rate even with no prior dealing," and therefore "the term reaches initial rates for new applicants."[100] However, the Court then looked to § 1681m(a), which "calls for notice only when the adverse action is 'based in whole or in part on' a credit report."[101] Here the Court held that "the phrase 'based on' indicates a but-for causal relationship and thus a necessary logical condition. Under this most natural reading of § 1681m(a), then, an increased rate

---

[95] 15 U.S.C. § 1681(a)(4) (2000 & Supp. V), *available at* http://uscode.house.gov/pdf/2005/2005usc15.pdf.

[96] Safeco Ins. Co. of Am. v. Burr, 127 S. Ct. 2201 (2007).

[97] *Id.*

[98] *Id*. at 2205, 2210.

[99] *Id*. at 2208–10.

[100] *Id.* at 2212.

[101] *Id.*

is not 'based in whole or in part on' the credit report unless the report was a necessary condition of the increase."[102] Since notice is not explicitly required for adverse action from merely consulting a report, the Court reasoned that conditioning the requirement on action "based on" a report suggests the duty comes from an actual consequence of reading the report, not just an event that would have happened anyway."[103]

The Court then determined the benchmark for whether setting a high first-time rate constitutes a disadvantageous increase, and would thus be an adverse action requiring notice. It held that the baseline rate should be the rate that "the applicant would have had if the company had not taken his credit score into account."[104] In reaching its conclusion, the Court determined that Congress was "more likely concerned with the practical question whether the consumer's rate actually suffered when the company took his credit report into account than the theoretical question whether the consumer would have gotten a better rate with perfect credit."[105] The Court then addressed the issue of whether a customer needs to be provided notice when the initial rate offered, if considered an increase, is consistently and repeatedly offered to the client at the beginning of each new dealing.[106] The Court held that such repeat notices were unnecessary, noting that:

> [o]nce a consumer has learned that his credit report led the insurer to charge more, he has no need to be told over again with each renewal if his rate has not changed. For that matter, any other construction would probably stretch the word 'increase' more than it could bear. . . . Once buyer and seller have begun a course of dealing, customary usage does demand a change for 'increase' to make sense. Thus, after initial dealing between the consumer and the insurer, the

---

[102] *Id.*

[103] *Id.*

[104] *Id.* at 2213.

[105] *Id.*

[106] *Id.* at 2214.

> baseline for 'increase' is the previous rate or charge, not the 'neutral' baseline that applies at the start.[107]

In the consolidated action of *GEICO General Insurance Company v. Edo*, the Supreme Court found that since the initial rate offered to Edo was the same it would have been had Edo's credit score not been taken into account, there was no need for GEICO to provide Edo with adverse action notice under § 1681m(a).[108] In *Safeco,* Safeco was found to have violated the FCRA by not providing adverse action notification when it used consumer credit reports to determine the initial application rate of Burr.[109] However, to be liable, Burr had to establish that Safeco had acted recklessly in its violation.[110] Since the Court found that Safeco's mistake in application of the term "increase" in the Act was not unreasonable, Safeco did not act recklessly by not providing adverse action notification and, therefore, was not liable.[111]

C. THE LEGITIMACY OF USING CONSUMER CREDIT REPORTS TO ASSESS ABILITY TO PAY

On June 22, 2006, the District Court for the Middle District of Alabama decided *Wallace v. Finkel.*[112] The issue in that case was whether respondent Finkel obtained petitioner Wallace's credit report for a permissible purpose under the FCRA.[113] The court ruled that respondent's use of a consumer credit report, without consent of the consumer, to assess the consumer's ability to pay for medical services did not violate the FCRA.[114]

The plaintiff claims that the purpose was improper because she did not intend to enter into a "credit transaction" with the defendant (i.e.

---

[107] *Id.*

[108] *Id.*

[109] *Id.* at 2215.

[110] *Id.*

[111] *Id.*

[112] Wallace v. Finkel, No. 2:06CV05-SRW, 2006 WL 1731149 (M.D. Ala. 2006).

[113] *Id.* at *2.

[114] *Id.* at *1.

did not initiate the transaction). Therefore, she argued, he had no legitimate purpose to assess her ability to pay. The court found that, although she did not intend to enter a "credit transaction", the plaintiff did initiate the overall transaction which was sufficient to meet that portion of the statute's requirements.[115]

The court had identified the release of the information to individuals who have "a legitimate business need for the information . . . in connection with a business transaction that is initiated by the consumer" as a permissible purpose under the FCRA.[116] Based on the principles of statutory interpretation, the court found that regardless of what the statute may say elsewhere, the "business need" as applied to the case at hand covered the respondent's circumstances based on previous FTC construction of the statute.[117] Accordingly, without any other evidence presented against the defendant, the court found no indication that the defendant accessed the consumer credit report for anything other than a legitimate business need covered under the FCRA.[118]

D. TARGETED MARKETING CAMPAIGNS AND THE FCRA: *MURRAY V. SUNRISE CHEVROLET, INC.*

On July 31, 2006, the United States District Court for the Northern District of Illinois decided *Murray v. Sunrise Chevrolet, Inc.*[119] The main issue in *Murray* was whether a notice of pre-approval constituted a firm offer of credit, creating a permissible purpose for respondent to access petitioner's credit report without written consent.[120] The court held that the respondent did in fact violate the FCRA when, during the course of a targeted marketing campaign, it both failed to get permission of consumers in Illinois and failed to extend them a firm

---

[115] *Id.*

[116] *Id.* at *3 (quoting 15 U.S.C. § 1681b(a)(3)(F)(i)).

[117] *Id.* at *4.

[118] *Id.* at *5–6.

[119] Murray v. Sunrise Chevrolet, Inc., 441 F. Supp. 2d 940 (N.D. Ill. 2006).

[120] *Id.* at 941–42.

offer of credit when it accessed their credit records.[121] The second issue presented was whether the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") prevented petitioner from bringing a private action against respondent.[122] The court held that the FACT Act does not apply retroactively, and the activities in the surrounding cause of action occurred prior to the enactment of the section of the FACT Act that would prevent petitioner's action.[123]

The court held that this action was covered under the FCRA, which mandates that access of a consumer credit report is allowed only with written consent of the consumer or for a permissible purpose, one such purpose being to make a firm offer of credit to the consumer.[124] This firm offer of credit is defined by the court as being, "any offer of credit . . . to a consumer that will be honored if the consumer is determined, based on information in a consumer report on the consumer, to meet the specific criteria used to select the consumer for the offer."[125] The offer that was extended by the defendant was not a firm offer, according to the court, because it was not an actual guarantee that the plaintiff would be granted the loan amount.[126]

The next issue examined by the court was whether the respondent provided a "clear and conspicuous notice" to the plaintiff of the right to prohibit the use of their credit report for such purposes as an auto loan solicitation under of FCRA.[127] The court found that respondent had not, holding that in order to comply with the clear and conspicuous requirements under the FCRA,

> The creditor must disclose that 1) it used information from the consumer's credit report in connection with the offer; 2)

---

[121] *Id.* at 950; For additional information, *see* Donald G. Aplin, *Court: Willful Violation Allegations are Viable in FCRA Class Claim over Car Dealer Mailings*, 5 PRIVACY & SEC. L. REP. (BNA) No. 33, at 1141 (Aug. 14, 2006).

[122] *Murray*, 441 F. Supp. 2d at 945.

[123] *Id.*

[124] *Id.* (citing 15 U.S.C. § 1681b(c)(1)(B)(i)). *See also* FTC, THE FAIR CREDIT REPORTING ACT, *available at* http://www.ftc.gov/os/statutes/fcradoc.pdf (last visited Jan. 29, 2008) (discussion on permissible purposes).

[125] *Id.* (quoting 15 U.S.C. § 1681a(1)).

[126] *Id.* at 947.

[127] *Id.*

> the consumer received the offer because she satisfied the creditor's criteria for credit worthiness; 3) failure to meet the section criteria or any applicable criteria bearing on credit worthiness may cause the creditor to rescind the offer; 4) the consumer has a right to prohibit her credit report from being used in connection with any credit transaction that she does not initiate; and 5) she may exercise her right to "opt out" of such credit transactions by contacting a specified toll-free number or by sending a written request to the credit agency at a given address.[128]

However, just because a creditor includes all these points on the document sent out to the consumer does not automatically guarantee that the document meets the clear and conspicuous test, as notice of the above information must be presented in a way that actively draws the attention of the consumer.[129] Because the defendant's pre-approval notice did not do this, the court held that it failed the clear and conspicuous test.[130]

The court also addressed the issue of whether it was possible for the plaintiff to establish that the defendant willfully violated the FCRA requirements, against the assertions of the defendant.[131] In order to show a willful violation, the court held that "Murray must be able to demonstrate that Triad and Sunrise 'knowingly and intentionally' violated the statute and in so doing, were 'conscious' that their acts 'impinge[d] on the rights of others.'"[132] However, due to the unavailability of information on the issue, for the purposes of summary judgment, the court declined to decide if the defendant acted willfully.[133]

---

[128] *Id.* at 947–48 (citing 15 U.S.C. § 1681m(d)(1)).

[129] *Id.* at 948.

[130] *Id.*

[131] *Id.* at 949.

[132] *Id.* (citation omitted).

[133] *Id.* at 950.

E. TARGETED MARKETING CAMPAIGNS AND THE FCRA: *MURRAY V. NEW CINGULAR WIRELESS SERVICES, INC.*

On May 22, 2006, the U.S. District Court of the Northern District of Illinois decided another targeted marketing campaign case, *Murray v. New Cingular Wireless Services, Incorporated*.[134] The issues presented were whether the defendant presented a firm offer and whether the defendant made a clear and conspicuous disclosure of the consumer's rights.[135] The court held that the defendant had indeed made a firm offer of credit as defined under the FCRA and was therefore not in violation of the Act when it accessed individual credit reports without first gaining permission from the individuals.[136] The court went on to find that while the defendant failed to meet the clear and conspicuous requirement under the FCRA, because the plaintiff could not show that Cingular willfully violated the FCRA, summary judgment was granted.[137]

The court reached the decision concerning whether the offer was a firm offer of credit by looking at all the circumstances surrounding the offer. It stated "[i]n making this determination, we must consider the amount of credit extended; whether the offer has value; whether approval was guaranteed; and the other terms of the offer, such as the rate of interest charged, the method of computing interest and the length of the repayment period."[138] When analyzing these circumstances, the court found that there was a firm offer because "the pre-approval for the new phone is tied to activation on a qualifying Cingular monthly wireless plan and is not simply pre-approval for a free wireless phone only."[139] Further supporting the holding was the fact that "consumers who sign up for a wireless phone plan are extended credit because they pay for service at the end of the month rather than buying the minutes in advance."[140] This characterization is

---

[134] 432 F. Supp. 2d 788 (N.D. Ill. 2006).

[135] *New Cingular Wireless Servs., Inc.*, 432 F. Supp. 2d at 790.

[136] *Id.* at 792.

[137] *Id.* at 793–94; *see also*, *Court Throws Out Consumer Class FCRA Suit over Wireless Offer Based on Credit Reports*, 5 PRIVACY & SEC. L. REP. (BNA) 24, at 835 (June 12, 2006).

[138] *New Cingular Wireless Servs., Inc.*, 432 F. Supp. 2d at 791.

[139] *Id.*

[140] *Id.*

within the definition of credit found under section 1691a(d) of the FCRA, which states that credit is "the right . . . to purchase property or services and defer payment therefore."[141] The court also supports its holding by stating that there is no indication that the offer is lacking a guarantee to be honored if the consumer decides to accept the offer, nor must there be an interest rate for the offer to be considered valid under the FCRA as a firm offer.[142]

However, the court did not find that the defendant likely complied with the clear and conspicuous requirement under the FCRA.[143] In the mailing sent out to the plaintiff, the only indication of the necessary disclosures was the term "DISCLOSURE" in capital letters.[144] This was found to be insufficient because, along with all other information included in the mailing, it was in extremely small font and therefore unlikely to draw the reader's attention.[145] This was not found to be fatal to the defendant's case, though, for while the court found that the disclosures likely failed the clear and conspicuous requirements, the court pointed out no case has yet definitively determined the meaning of "clear and conspicuous."[146] Therefore, since the defendant was found to have made a firm offer and the plaintiff was unable to show a willful violation of the FCRA, the court ruled that the plaintiff's case must fail and ruled for the defendant on its motion for summary judgment.[147]

F. CONCLUSION

While *Safeco Insurance Company of America v. Burr* and *GEICO General Insurance Company v. Edo* are the only two cases that present binding case law in the area of the FCRA, the other cases are not insignificant. How the Supreme Court handles the decisions of the lower courts in these cases could have a great affect on the future

---

[141] *Id.*

[142] *Id.* at 792.

[143] *Id.* at 793.

[144] *Id.*

[145] *Id.*

[146] *Id.* at 794.

[147] *Id.*

interpretation of the FCRA. As such, it will be imperative to monitor these cases and cases that cite them to see how the Supreme Court rules on the interpretations these cases propose.

V. CONCLUSION

The revelation of the U.S. government's use of the SWIFT database to track the financial transfers of terrorist organizations is one of the most important developments in financial privacy law this year. Its implications are monumental, not only for the continuing success of the U.S. in fighting terrorism, but also for EU privacy law and the U.S. freedom of the press. Although the information was released in June 2006, the issue is far from fading. Much is yet to be seen regarding how the EU will respond to SWIFT's compliance with the U.S. subpoena and whether the U.S. Congress will restrict the free speech of the American press. As such, this issue should be watched vigilantly in the coming months.

While much of the media focused mainly on the SWIFT leak and subsequent developments, it was not the only important development in the area of financial privacy this year. The Grahm-Leach-Bliley Act was also an area of significant development. The amendments to GLBA via section 609 of the Financial Regulatory Relief Bill signed into law October 13, 2006, will reduce CPAs federally mandated workload. Additionally, the Mississippi Supreme Court's decision in *Capital One Services, Inc. v. Page* presents the issue of what exactly are the exceptions to the nondisclosure rule of the GLBA, an issue that has yet to be addressed by the U.S. Supreme Court. Finally, the issues of whether lawyers are service providers and proposed changes in privacy notices are both being addressed by professionals in the financial privacy realm. We should expect major changes in the future regarding these issues.

Significant developments regarding the Fair Credit Reporting Act also deserve attention. The Supreme Court's holdings in *Safeco Insurance Company of America v. Burr* and *GEICO General Insurance Company v. Edo* provide additional interpretation of the provisions of the FCRA regarding what is required for a finding of an "adverse action," which is needed to bring suit under the FCRA. In addition, the district courts tackled several aspects of FCRA, including what is viewed as a legitimate business need, what is considered a firm offer of credit, what counts as "clear and conspicuous notice," what constitutes a "firm offer," and what is a willful violation of the FCRA. However, none of the district court cases are binding. We must await future Supreme Court decisions

before these and other issues of financial privacy law in the United States are clear. These developments concerning FCRA, however, as well as the ones concerning GLBA and the SWIFT database, demonstrate just how turbulent a year it has been in the world of financial privacy.