Two-Factor Authentication: A Solution to Times Past or Present? The Debate Surrounding the Gramm-Leach-Bliley Security Safeguards Rule and the Methods of Risk Assessment and Compliance

RITU SINGH*

ABSTRACT

Recently, security of consumer information in financial institutions has become more of a concern to consumers alongside financial institutions. In response, the government has enacted the Gramm-Leach-Bliley Act. This Act contains a notable Security Safeguards Rule. Financial institutions, a term broadly defined in the Act, are to comply through risk assessment procedures and implementation of appropriate security measures. A debate exists as to whether two-factor authentication (1) should be the minimal level of compliance and (2) whether it is indeed the best solution. While some may argue that currently it provides a "best" solution, such a solution is not foolproof. Two-factor authentication may address issues that arrive through one-factor authentication, such as password guessing. It is not adequate, however, in addressing the more active nature of attacks today that occur through phishing and Trojan horses. Also, two-factor authentication goes beyond the minimal standards required across a broad scope of financial institutions. The Gramm-Leach-Bliley Act is meant to cover financial institutions with varying levels of appropriate risk assessment and security measures. A mandate of two-factor authentication would go beyond the purpose of the Act to implement minimum standards across a broad scope of financial institutions. While arguably an effective solution in today's world, if one that may go beyond minimal compliance, two-factor authentication is not an end solution as it simply addresses the passive attacks of yesterday and not the more active attacks of today and the future.

I. EXISTING LEGISLATION: THE GRAMM-LEACH-BLILEY ACT AND SECURITY SAFEGUARDS

Security has always been a concern of the federal government. Only recently, however, has it become a concern for consumers in

* Ritu Singh is a third-year law student at The Ohio State University Moritz College of Law. Ritu received a B.S. in industrial engineering, and economics, and a Business Basics Certificate from Northwestern University.

regard to the consumer information kept by financial institutions. In the electronic and Internet banking worlds of today, these institutions are easy prey to identity theft if security measures are not in place. To address these concerns and provide further guidance to financial institutions as to what is an adequate security system, Congress passed the Financial Modernization Act of 1999, otherwise known as the Gramm-Leach-Bliley Act ("GLB"). GLB "regulates the privacy and protection of customer records maintained by financial institutions."[1]

The statute sets forth a congressional policy stating 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."[2] Moreover, the statute gives agencies regulating financial institutions the responsibility of setting forth appropriate standards. The standards are to relate to technical, administrative, and physical safeguards for the following objectives:

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.[3]

GLB defines "financial institution" broadly. Besides banks, the scope of this term also includes credit unions, credit-card issuing companies, mortgage loan companies, broker/dealers, and other institutions that interact with consumers through means of financial

---

[1] Daniel J. Langin, *Gramm-Leach-Bliley Security Requirements: Keeping Robbers and Regulators from the Door*, Recourse Technologies at 1 (2002), *available at* http://www.securitymanagement.com/library/gramm_tech0902.pdf.

[2] Financial Modernization Act (Gramm-Leach-Bliley) Act of 1999, 15 U.S.C. § 6801(a) (2005).

[3] 15 U.S.C. § 6801(b) (2005).

transactions with them or through providing financial services or products to them.[4]

As a result of GLB, and specifically the security safeguards requirement section, the requisite agencies[5] issued the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information," commonly referred to as "the Guidelines."[6] The Guidelines created common standards across financial institutions to address security issues. A letter from the Federal Reserve System, dated May 31, 2001, further explained the procedure for examining compliance, stating that financial institution examiners are required to "assess compliance with the Guidelines during *each safety and soundness examination cycle* (which may include *targeted reviews of information technology*) . . . and *monitor ongoing compliance* as needed."[7]

In total, the Guidelines require "the development and implementation of security programs that: [i]nvolves the Board of Directors, [a]ssesses risk, [m]anages and controls risk, [o]versees service provider arrangements, [a]djusts the program, [r]eports to the Board, [and] [i]mplements the standards."[8] A violation of these standards is a serious offense and may result in a daily fine anywhere from $5,000 to $1,000,000.[9]

---

[4] *See* FTC Privacy of Consumer Financial Information, 16 C.F.R. § 313.3(k)(2) (2001).

[5] The Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency, Office of Thrift Supervision and the National Credit Union Administration. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 1 (2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf [hereinafter Guidelines].

[6] Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8616 (Feb. 1, 2001) (to be codified at 12 C.F.R. pts. 30, 208, 211, 225, 263, 308, 364, 568, 570); *see also* Langin, *supra* note 1.

[7] Letter from Richard Spillenkothen, Director, Board of Governors of the Federal Reserve System, to The Officer in Charge of Supervision and Appropriate Supervisory and Examinations Staff at Each Federal Reserve Bank and to Each Domestic Banking Organization Supervised by the Federal Reserve System (May 31, 2001) (emphasis added), *available at* http://www.ffiec.gov/exam/InfoBase/documents/02-frb-privacy-sr01-15(sup)010531.pdf; *see also* Langin, *supra* note 1.

[8] JAMES WEISSMAN, GLOBAL INFORMATION ASSURANCE CERTIFICATION, MAKING THE CASE FOR MANAGED SECURITY 5 (2004), *available at* http://www.giac.org/certified_professionals/practicals/gsec/3889.php.

[9] *Id.*

The security breaches of 2005, notably those at data brokers LexisNexis and ChoicePoint,[10] were strong incentives for the creation of the Guidelines. The Guidelines set forth "certain affirmative obligations aimed at protecting sensitive financial information and notifying customers in the event of a security breach."[11] Pursuant to the GLB Safeguards Rule, the Guidelines were collectively issued by the Federal Financial Institutions Examination Council ("FFIEC") agencies. [12] FFIEC agencies issued the updated guidance with the specific objective to address "why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services."[13]

An onus is placed on financial institutions to create a strong IT environment which addresses security issues such as "unauthorized disclosure of information, misuse of data, and alteration or destruction of personal data."[14] To accomplish these goals, many financial institutions created programs that incorporated a strong identity and access management ("IAM") system.[15]

Single-factor authentication in terms of password-centric security currently complies with the Guidelines. There is a push, however, for strong authentication, also known as two-factor authentication, to be

---

[10] *Id.* (The public only became informed of these breaches due to an existing California law requiring consumers be notified upon such an event).

[11] *Examining the Financial Industry's Responsibility to Prevent Identity Theft and Protect Sensitive Consumer Financial Information: Hearing Before the S. Comm. on Banking, Housing and Urban Affairs*, 109th Cong. 4 (1st Sess. 2005) (statement of Ira D. Hammerman, Senior Vice President and General Counsel, Securities Industry Association), *available at* http://banking.senate.gov/_files/hammerman.pdf (last visited Sept. 30, 2006); *see also* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736-54 (Mar. 29, 2005) (to be codified at 12 C.F.R. pts. 30, 208, 225, 364, 568, 570).

[12] Guidelines, *supra* note 5, at 1.

[13] *Id.*

[14] *Strong User Authentication and Gramm Leach Bliley: Cost-Effective Compliance with Title V Privacy Provisions*, BIOPASSWORD, Mar. 2004, at 4, *available at* http://www.verticalcompany.com/pdfs/BioPassword-Graham%20Leach%20Bliley.pdf.

[15] *Id.*

the standard in these financial institutions as well as among consumers.[16]

The FFIEC Guidance has created, in what some believe to be more a mandate than guidance, that "[s]tarting in January 2007, financial institutions *must* provide consumers of online financial services with the same security protection enjoyed by customers buying groceries or gas with a debit card: strong authentication."[17] The specific FFIEC statement provides: "Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions *should* implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks."[18] As this paper shall discuss, however, strong authentication is not an end solution. Further, mandatory implementation of strong authentication goes beyond the purpose of GLB of applying minimal standards across the broad scope of companies held to be "financial institutions."

II. ENFORCEMENT OF GLB AND FAILURE OF COMPLIANCE

In order to assess the risks properly and implement appropriate safeguards, a certain level of compliance must be understood and met by financial institutions. Again, the definition of financial institutions that must comply with the safeguards is broad. This definition even stretches to include the automotive industry due to vehicle transaction financing aspects. A report to the automotive industry recommending what is necessary for compliance with the GLB Safeguards directs the industry to

> develop, implement, and maintain a *comprehensive information security program* . . . [which] must be *in writing* and it must be *readily accessible* . . . [and] must contain *administrative, technical, and physical safeguards* that are appropriate to [the] size and complexity [of the financial

---

[16] "Strong means two or more types of identity verification in return for access." *See* Scott Berinato, *Second Thoughts on Second Factors: Seven Ways in Which a New Strong-Authentication Standard isn't Quite What It Appears to Be*, CSO (Feb. 2006), http://www.csoonline.com/read/020106/second_thoughts.html.

[17] *Id.* (emphasis added).

[18] Guidelines, *supra* note 5, at 4 (emphasis added).

> institution], the nature and scope of [their] activities, and the sensitivity of any customer information at issue.[19]

The report further states that while the Safeguards Rule does prescribe five essential elements of compliance that financial institutions must address in a written, comprehensive information security program, any further identification of "meaningful, concrete security measures falls to the party with the best access to information . . . about risks[]"—the financial institution itself.[20]

Accounting for the fact that different risks may be applicable to different financial institutions, the Federal Trade Commission ("FTC") built a level of flexibility into what is required for financial institutions to comply with the GLB Safeguards. The five required elements the FTC set forth include the following:

1. Designate an employee or employees to coordinate your information security program.

2. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of [the financial institution's] operations, including:

    a. Employee training and management;

    b. Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

---

[19] REYNOLDS & REYNOLDS, UPDATE: COMPLYING WITH THE GRAMM-LEACH-BLILEY ACT PRIVACY AND SAFEGUARD RULES 1 (Jan. 2004), http://www.reyrey.com/Gramm_Leach_Bliley_Act_Brochure.pdf.

[20] *Id.*

c. Detecting, preventing, and responding to attacks, intrusions, or other system failures.

3. Design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguard's key controls, systems, and procedures.

4. Oversee service providers by:

   a. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

   b. Requiring [by contract that] service providers implement and maintain such safeguards.

5. Evaluate and adjust [the financial institution's] information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any circumstances that you know or have reason to know may have a material impact on your information security program.[21]

The report further summarizes these five elements into useful recommendations. These recommendations are listed below:

1. "Coordinate with your coordinator."[22]

2. Focus on the risks that matter at that particular financial institution and recall that the Safeguards do not require

---

[21] *Id.*; *see also* FTC, Financial Institutions and Customer Data: Complying with the Safeguards Rule, FTC FACTS FOR BUSINESS, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf (last visited Sept. 30, 2006) [hereinafter FTC FACTS FOR BUSINESS].

[22] REYNOLDS & REYNOLDS, *supra* note 19, at 1.

mitigation of remote risks but do require reasonably assessed ones.[23]

3. Maximize efficiency of your safeguards contract by minimizing risk of duplicate contracts of this nature in the financial institution, perhaps by designating one person to receive copies from all departments of safeguards contracts.[24]

4. "Keep pace;"[25] as the FTC states, "[b]ecause of the ever-changing nature of the relevant risks, however, the Commission does not find it appropriate to delineate risks more specifically within the Rule."[26]

As to the final point regarding compliance with the Safeguards, assessing and focusing on current risks is not enough. The financial institutions must keep up to date with the ever changing world of risks and intercept these risks in order to maintain compliance. Security measures must address current issues and also be able to address evolving issues for the future because "[a] slow reaction to changing vulnerabilities will widen the window of opportunity for a successful attack."[27]

A. GLB ENFORCEMENT AGAINST NATIONWIDE AND SUNBELT

In the fall of 2004, the FTC conducted a nationwide compliance sweep that resulted in the formal charging of two mortgage companies, both falling under the GLB definition of "financial institutions." These two companies, Nationwide Mortgage Group, Inc.

---

[23] *Id.*

[24] *Id.* at 2.

[25] *Id.*

[26] Standards for Safeguarding Customer Information: Final Rule, 67 Fed. Reg. 36,489, 36,489 (May 23, 2002) (to be codified at 16 C.F.R. pt. 314), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf (last visited Sept. 30, 2006); *see also* FTC FACTS FOR BUSINESS, *supra* note 21.

[27] REYNOLDS & REYNOLDS, *supra* note 19, at 2.

("Nationwide") and Sunbelt Lending Services, Inc. ("Sunbelt"), were the first companies that the FTC enforced the Safeguards Rule against.[28]

The FTC alleged that Nationwide and its President, John D. Eubank, had "failed to implement safeguards to protect . . . customers' names, social security numbers, credit histories, bank account numbers, income tax returns, and other sensitive financial information."[29] Mainly, Nationwide failed to employ training on Internet security, oversee how customer information was handled by its loan officers, and to make sure to catch vulnerabilities in its computer network through proper monitoring techniques. Sunbelt faced similar charges as it "also failed to oversee the security practices of its service providers and of its loan officers" and agreed to settle with the FTC with an agreement barring future Safeguards Rule violations and a requirement of biannual audits of the information security program at Sunbelt for ten years by a qualified and independent professional.[30] Nationwide, too, agreed to settlement terms to not violate the GLB Act any further, and to utilize "a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for ten (10) years after service of the order."[31] Guidelines would be set forth for Nationwide to implement, follow, and assess for compliance purposes according to Nationwide's size and complexity. Nationwide would also be responsible to uphold assurances that the program operates in such a manner that "the security, confidentiality, and integrity of personal information is protected."[32]

As a result of the initial sweep, the FTC declared that both companies had failed to comply with the Safeguards Rule's basic requirements. More specifically, they did not "assess risks to sensitive

---

[28] Press Release, FTC, FTC Enforces Gramm-Leach-Bliley Act's Safeguards Rule Against Mortgage Companies (Nov. 16, 2004), *available at* http://www.ftc.gov/opa/2004/11/ns.htm.

[29] *Id.*

[30] *Id.*

[31] Nationwide Mortgage Group, No. 9319, 2005 F.T.C. LEXIS 55, at *3 (2005), *available at* http://www.ftc.gov/os/adjpro/d9319/050415dod9319.pdf.

[32] *Id.*

customer information [and] implement safeguards to control these risks."[33] Guidance had been available for the companies to consult in order to determine how to comply properly with GLB Safeguards Rule.

The FFIEC Guidance ("[c]onsistent with the *FFIEC Information Technology Examination Handbook*, Information Security Booklet, December 2002") includes a risk assessment process. In this section, they communicate three points of the process:

- Identify all transactions and levels of access associated with Internet-based customer products and services;
- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and
- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.[34]

The FFIEC communicated to examiners how to conduct inspections in the various fields to maintain a level of consistency. While examiners do not require two-factor authentication to be in place (as the guidances are risk-based rather than technology specific), they do look at a combination of how financial institutions address the interplay of risks, their customer preferences, and the market.[35] However, the FFIEC has not yet taken a firm position on what exact

---

[33] Posting of Camelia Mazard, FTC Consumer Protection Highlights to Antitrust Law Blog, http://www.antitrustlawblog.com/highlights-84-ftc-consumer-protection-highlights.html (Mar. 8, 2005).

[34] Guidelines, *supra* note 5, at 2, 4.

[35] Interview with John Carlson, Senior Director, BITS, in Washington, D.C. (Jan. 19, 2006) (on file with author).

type of security, front-end or back-end, should be implemented by financial institutions.[36]

III. PRIVACY AND SECURITY LEGISLATION AND STATE INITIATIVES

A wide variety of proposed legislation addressing security in the information age has been put forth, especially in response to many of the security breaches which occurred over the past year, such as breaches at data brokers ChoicePoint and LexisNexis. Most notably, one of these is the Information Protection and Security Act, S. 500 and H.R. 1080 of the 109th Congress.[37] This legislation, proposed by Sen. Bill Nelson (D-Fla.) and Rep. Edward Markey (D-Mass.), would regulate data brokers.[38] Groups such as the U.S. Public Interest Research Group ("PIRG") take a strong interest in the passage of this Act as it would impose "Fair Information Practices (FIPs) based rules on information brokers, [allow] consumers to enforce the law and [allow] states to continue to enact stronger laws."[39]

States have been active in their legislative reform regarding the privacy and security issue. California itself has taken strong action since 1999 through forty new privacy initiatives.[40] Indeed, Sen. Dianne Feinstein (D-Calif.) proposed as recently as April 2005 a more tightened, stricter version of her ID Notification bill, which would close loopholes found in S.B. 1386, or rather, California's notification law.[41]

In fact, only through California's enactment of security breach disclosure legislation was the ChoicePoint loss of information even discovered by consumers (through required consumer notification

---

[36] Isabelle Lindenmayer, *FFIEC Advisory Reopens An Old Security Debate*, AM. BANKER 6-9, Oct. 31, 2005, *available at* http://www.netbankaudit.com/images/American_Banker_on_Authentication.pdf.

[37] H.R. 1080, 109th Cong. (2005); S. 500, 109th Cong. (2005).

[38] Lisa Vaas, *Two-Factor Authentication Could Stem Rising Tide of Identity Theft*, EWEEK.COM, Apr. 15, 2005, http://www.eweek.com/article2/0,1759,1787134,00.asp.

[39] Letter from PIRG to Senator Nelson and Representative Markey (Mar. 8, 2005), http://www.pirg.org/consumer/pdfs/pirgendorsesnelsonmarkey.pdf.

[40] Gwen Kennedy, *Thumbs Up for Biometric Authentication!*, 8 COMP. L. REV. & TECH. J. 379, 396 n.73 (2004).

[41] *See* Vaas, *supra* note 38.

upon the loss of their information).[42] After this security breach, PIRG noted that "a dozen states or more are now considering security breach proposals, security freeze proposals (which allow consumers to 'freeze' access to their reports to new users, and have already been enacted in California, Texas, Louisiana and Vermont) and other reforms."[43] However, while California and Texas enacted laws covering all consumers, Louisiana and Vermont only enacted the laws for identity theft victims. After the ChoicePoint and LexisNexis security breaches, which again the public was informed of only as a result of the California law, over twenty-seven states in 2005 ended up filing state security freeze bills, while California and Texas went on to further file bills which would strengthen their existing laws.[44]

State action is proceeding quickly on the issue, as seen in the more than doubling of states with enacted security freeze laws alone within the first months of 2006. In an update posted January 4, 2006, the PIRG reported that "there are now a total of twelve states with laws allowing consumers to restrict access to their credit reports."[45] The states with enacted security freeze laws for all consumers included California, Colorado, Connecticut, Louisiana, Maine, Nevada, New Jersey, and North Carolina.[46] The states with enacted security freeze

---

[42] Letter from PIRG to Senator Nelson and Representative Markey, *supra* note 39.

[43] *Id.*; *see also* the PIRG/Consumers Union State Model Identity Theft Law, The State Clean Credit and Identity Theft Protection Act, *available at* http://www.pirg.org/consumer/credit/model.htm (last visited Sept. 30, 2006).

[44] *Identity Theft Shenanigans Cloud End of Legislative Session*, THE AKPIRG ADVOCATE, June 2006, http://www.akpirg.org/Publications/Newsletters/June2006newsletter.pdf; *see generally State PIRG Summary of State Security Freeze and Notification Laws*, Update as of July 18, 2006, http://www.pirg.org/consumer/credit/statelaws.htm (last visited Sept. 30, 2006).

[45] THE AKPIRG ADVOCATE, *supra* note 44, at 3.

[46] *State PIRG Summary of State Security Freeze and Notification Laws*, *supra* note 44. *See also* Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft: Before the S. Comm. on Banking, Housing and Urban Affairs, 109th Cong., 23 (2005) (testimony of Consumer and Privacy Groups on Security Breaches and Privacy, Edmund Mierzwinski, U.S. PIRG Consumer Program Director) ("The New Jersey General Assembly has passed what will be the strongest freeze law in the country. The bill allows all consumers to use the security freeze tool at a minimal cost and requires the credit bureaus to facilitate the quick placement and lifting of the freeze."); California (CAL. CIV. CODE §§1785.10-1785.19.5 (Deering 2003)), Colorado (Sen Bill 05-137; *available at* http://www.leg.state.co.us/Clics2005a/csl.nsf/fsbillcont3/349195C4D17F1A7787256F8E0001202B?Open&file=137_enr.pdf), Connecticut (2005 Conn. Pub. Acts 148), Louisiana (2004

laws for identity theft victims rather than all consumers included Illinois, Vermont, Texas, and Washington (where Washington further includes victims of security breaches).[47] Moreover, the PIRG stated that other bills still to pass during the year were being considered in California, Delaware, Maine, Michigan, New York, and Oregon.[48]

On July 18, 2006, the PIRG updated its information on state legislation of security freeze and security breach notification laws.[49] In the first half of 2006, the number of states giving the right to a security freeze to all state residents increased from eight to twenty.[50] Of the other four states, which had simply provided security freeze rights to identity theft victims as of January 2006, two of those states, Vermont and Illinois, have now expanded the right to all consumers.[51] Additional states to enact security freeze laws for identity theft victims alone are Hawaii, Kansas, and South Dakota.[52]

In total, as of July 18, 2006, "[twenty-five] states have enacted legislation that either already grants or will soon give all or some consumers the right to prevent identity theft by placing a security freeze on their credit reports."[53] Within the first half of 2006, the amount of states with security freeze laws more than doubled from twelve to twenty-five states.

La. Acts 766), Maine (LD 581), Nevada (2005 Nev. Stat. 391), New Jersey (2005 N.J. Laws 226), North Carolina (2005 N.C. Sess. Laws 414).

[47] *State PIRG Summary of State Security Freeze and Notification Laws*, *supra* note 44 (Illinois (2005 Ill. Laws 74), Vermont (2004 Vt. Acts & Resolves 155), Texas (2003 Tex. Gen. Laws 1326), and Washington (2005 Wash. Sess. Laws 342)).

[48] *Id.* (States to have considered security freeze bills in 2005 include: Arkansas, California, Delaware, Hawaii, Indiana, Kansas, Kentucky, Maryland, Maine, Michigan, Minnesota, Montana, New Mexico, Nevada, New York, Oregon, Pennsylvania, Rhode Island, Texas, South Carolina, and Utah).

[49] *State PIRG Summary of State Security Freeze and Notification Laws*, *supra* note 44.

[50] *Id.* (Additional states to the initial eight providing the security freeze right to all consumers now include Delaware, Florida, Kentucky, Minnesota, New Hampshire, New York, Oklahoma, Rhode Island, Utah, and Wisconsin).

[51] *Id.*

[52] *Id.*

[53] *Id.*

Other security bills were considered and enacted over 2005 as well, such as the security breach notification laws introduced in at least thirty-five states and enacted in twenty-three states.[54] As of July 18, 2006, within the first half of 2006, the PIRG reports "at least [thirty-four] states have passed security breach notification laws."[55] Additionally, in the spirit of enhanced security measures, some state legislatures have considered bills specifically dealing with biometric information sharing, such as those in California,[56] New Jersey,[57] and Massachusetts.[58] These bills would regulate biometric information collection and distribution through means of a consumer consent requirement and a restriction on disclosure to certain third parties for purposes other than identification.[59]

Concerns over security breaches have gone beyond financial institutions to the consumers they serve. Many financial institutions may be heading towards two-factor authentication on their own to guarantee stronger compliance with the Guidelines. Yet John Carlson,

---

[54] State PIRG Summary, *supra* note 44, (Arkansas: Act 1526, *available at* http://www.arkleg.state.ar.us/ftproot/acts/2005/public/act1526.pdf, California (CAL. CIV. CODE §§1798.29, 1798.82-1798.84 (Deering 2005), Connecticut (2005 Conn. Pub. Acts 148), Delaware (75 Del. Laws 61 (2005)), Illinois (2005 Ill. Laws 36), Louisiana (2005 La. Acts 499), Minnesota (2005 Minn. Laws 167), Montana (2005 Mont. Laws 518), Nevada (2005 Nev. Stat. 485), New Jersey (2005 N.J. Laws 226), New York (2005 N.Y. Laws 491), North Carolina (2005 N.C. Sess. Laws 414), North Dakota (2005 N.D. Laws 447), Ohio (2005 HB 104), Pennsylvania (2005 Pa. Laws 94), Rhode Island (2005 R.I. Pub. Laws 225), Tennessee (security notification: H.B. 2178, S.B. 2227- but taken off committees; security freeze: H.B. 2480, filed for intro on Jan. 12, 2006), and the following other states: Washington, Florida and Texas); Applying to data brokers only: Georgia (2005 Ga. Laws 163); Applying to state agencies only: Indiana (2005 Ind. Acts 91); Applying to Information brokers only: Maine (2005 Me. Laws 379)).

[55] State PIRG Summary, *supra* note 44, (Additional states enacting security breach notification laws in 2006 include: Arizona, Colorado, Hawaii, Idaho, Kansas, Nebraska, New Hampshire, Oklahoma (state agencies only), Utah, and Wisconsin).

[56] S.B. 71, 1999-00 Leg., Reg. Sess. (Cal. 1999) (the bill failed in the Judiciary Committee).

[57] The Biometric Identifier Privacy Act, AB 2448, Leg., 210th Sess. (passed in the Assembly, September 23, 2002, received in the Senate, and referred to the Senate Judiciary Committee, September 26, 2002).

[58] H.B. 4483, 181st Gen. Ct., 1999 Reg. Sess. (Mass. 1999) (the bill passed just one house).

[59] Kennedy, *supra* note 40, at 395-97.

Senior Director of BITS,[60] notes, "It's easy to apply two-factor authentication when you have employees [or a government mandate] . . . . But it's a highly different equation when you deal with customers that can choose between different financial institutions."[61] Further, as Carlson has recently stated, "Based on a survey of BITS members in February 2005, the primary issue with two-factor is consumer acceptance/ease of use followed by cost, and technology issues (e.g., integration with existing IT systems)."[62]

IV. TWO-FACTOR AUTHENTICATION AS A CONSUMER SOLUTION AGAINST SECURITY BREACHES WITHIN FINANCIAL INSTITUTIONS

Two-factor authentication is mainly referred to regarding the use of "a small, digital token device to provide users with a random, six-digit code that changes every [sixty] seconds."[63] In order to access sites, for instance, online banking accounts, the user will use this unique code in combination with her user ID and password.[64]

A debate exists as to whether two-factor authentication is truly the key to solving the problem of identity theft, a problem greatly troubling both financial institutions and the consumers they serve. While many believe it to be the key, others are not so optimistic. As John Carlson states, "[t]wo factor can be a helpful tool. I would not go so far as to say it's the best solution. It has [to] be viewed in the context of entire information security program of a financial institution and the 'customer experience.'"[65]

Similarly, some such as Howard Schmidt, former special advisor to the President for cyber-space security, see two-factor authentication as a possible solution, but not the best one.[66] Schmidt believes that,

---

[60] Interview with John Carlson, *supra* note 35. John Carlson was also one of the authors of the GLB Guidelines for Safeguarding Customer Information.

[61] *See* Vaas, *supra* note 38.

[62] Interview with John Carlson, *supra* note 35.

[63] *See* Vaas, *supra* note 38.

[64] *Id.*

[65] Interview with John Carlson, *supra* note 35.

[66] Vaas, *supra* note 38.

rather than new laws, the solution would be to increase the amount of law enforcement personnel. Schmidt views two-factor authentication as only helping to reduce the number of victims, and not helping to stem the problem in the same manner that resources in law enforcement would (which, according to Schmidt, is what is actually needed).[67]

Bruce Schneier represents another voice on the issue. Schneier, an internationally renowned security technologist and author, wrote an essay depicting two-factor authentication as an outdated solution not capable of solving the problems existing in security today.[68] Schneier explains that the problem with passwords, and why many are pushing forward two-factor authentication rather than a single-factor authentication password method, is that they are easy to forget or lose.[69] Schneier does admit that two-factor authentication mitigates this problem; however, another problem exists as the nature of the attacks over the last decade has shifted from passive to active. Rather than simply being concerned with passive eavesdropping and offline password guessing, consumers and financial institutions of today are more concerned about active attacks in the form of phishing and Trojan horses.[70]

Phishing occurs through consumer fraud. For instance, a perpetrator will create a false website imitating a real bank's website in order to entice a user to type in her password so that the perpetrator can use it at the actual bank website. The user is unaware of the fraud and is either disconnected or passed on to the actual bank website to conduct a real transaction simultaneously with the perpetrator's fraudulent one.[71]

Trojan horses, rather, follow a different course. First, the perpetrator installs a Trojan on the user's computer. From then on,

---

[67] *Id.*

[68] Schneier on Security, *The Failure of Two-Factor Authentication*, http://www.schneier.com/blog/archives/2005/03/the_failure_of.html (Mar. 15, 2005) ("It won't defend against phishing. It's not going to prevent identity theft. It's not going to secure online accounts from fraudulent transactions. It solves the security problems we had ten years ago, not the security problems we have today.").

[69] *See id.*

[70] *Id.*

[71] *Id.*

upon user login at an actual bank website, the perpetrator may "piggyback" on the session in order to gain access to the user accounts so that fraudulent transactions might be made.[72]

Schneier, after laying out these new, "active" security concerns, describes how two-factor authentication will not solve these new problems. Schneier states that "[i]n the first case [of phishing], the attacker can pass the ever-changing part of the password to the bank along with the never-changing part. And in the second case [of Trojan horses], the attacker is relying on the user to log in."[73] He concludes with stating that the only true effect of two-factor authentication in addressing these security concerns would be to force criminals to modify their strategies. In his view, two-factor authentication will not be useless for those initial adopters of strong authentication (during the period the criminals are being forced to modify their behavior), for local logins, and with some corporate networks. Schneier does believe, however, that two-factor authentication will be useless for remote authentication over the Internet.[74]

In contrast, there are still those who believe the opposite, that two-factor authentication will not only play a role, but will play a strong one in cyber-security. One of those holding this belief is John McNulty, as he notes in his article responding to Schneier's essay.[75] While noting that Schneier's essay did address valid concerns in the banking IT security community, McNulty stated that he would not share Schneier's view of two-factor authentication being a failure rather than a solution. McNulty stresses that two-factor authentication addresses the serious concern of the vulnerability presented by traditionally fixed passwords, easily lost or stolen. Two-factor authentication is stated to be more secure simply as it requires two factors: "typically a PIN and a device such as a hardware token, which together generate a unique one-time-only passcode."[76] McNulty states that this will foil password theft as, a point on which Schneier agrees

---

[72] *Id.*

[73] *Id.*

[74] Schneier on Security, *supra* note 68.

[75] John McNulty, *Two-Factor Authentication is Still Strong*, EWEEK.COM, Apr. 11, 2005, http://www.eweek.com/article2/0,1759,1782435,00.asp.

[76] John McNulty, *News and Product Updates: Knock-Knock . . . Who's There?*, SECURE COMPUTING, May/June 2005, http://www.securecomputing.com/index.cfm?skey=1428.

as well, the intercepted password will not be good for the next login.[77] However, what McNulty fails to truly address and consider is the fact that criminals are active in today's world, continuously strategizing and generating methods to overcome such foils in their ever ongoing pursuit of identity theft.

Of particular interest, McNulty does not further address the Schneier explanation of why two-factor authentication still does not solve part of the phishing problem. Through phishing, during a transaction the attacker can still pass both parts of the password, the ever-changing and never-changing parts, to the bank. Moreover, McNulty responds to the concern of vulnerability of two-factor authentication to the more active cyber-security issues of the day, arising from the phishing and Trojan horse schemes Schneier outlines. His response, however, is simply that two-factor authentication will actually lead attackers to search for softer targets.[78] McNulty does not seem to consider that attackers might modify their strategic behavior. Rather, he appears to believe that the attackers will give up and move to targets which are not using the two-factor authentication approach. Further, to support his argument, and apparently weaken Schneier's, McNulty rests upon the fact that, for two decades, thousands of security conscious companies have successfully been using two-factor authentication in order to prevent identity thieves in action.[79] The key issue that McNulty bypasses, however, is Schneier's statement that two-factor authentication would solve the more passive cyber-security concerns of a decade past and not the more active ones we are facing in the present and in the future.

Two-factor authentication as a solution, or even the best solution, to attacks on consumer information is highly debated in today's world. One thing that both sides of the debate do appear to agree upon is that no security tool or system is foolproof.[80] Further, an arguable "best" solution of today may not be the "best" solution of tomorrow as attackers are constantly working to modify their strategies.

---

[77] McNulty, *supra* note 75.

[78] *Id.*

[79] *Id.*

[80] *Id.*

V. CONCLUSION

Two-factor authentication, though currently a useful tool for many financial institutions, will soon be facing the same level of cyber-security breach concern associated with single-factor, or rather password, authentication. Furthermore, while it has proven to be useful in some capacity, it will not be a useful tool for the remote user looking to improve cyber-security when conducting such business, such as online banking. In this ever-changing world of security risk, financial institutions will need to enact security programs to adapt to the more active risks of today to protect sensitive customer information. Financial institutions will need to provide consumers adept security measures to counteract those risks.

Unfortunately, the currently recommended tool of two-factor authentication appears to have reached its sunset as it is only truly capable of adequately addressing those passive security risks of days past. Simultaneously, however, legislation is finally being enacted to enforce security in financial institutions at a statewide level and to notify consumers of such security breaches. The awareness that should arise in the public as a course of this legislation should provide enough of a push for the financial institutions to continually adapt their security programs. This push will advance them to meet the risks of the days to come rather than settle into a comfortable pattern of minimal compliance. Without such a push, financial institutions may be satisfied in achieving minimal compliance with the GLB Safeguards Rule of today and then rest on meeting the demands of tomorrow. Hopefully, public awareness will not allow the sun to set on advancements in security improvements simply because some believe an end solution already exists in the form of two-factor authentication.