Recent Federal Developments

in Privacy and Information Security

Practising Law Institute

Tenth Annual Institute on Privacy and Security Law

New York City

June 22-23, 2009

Chicago

July 20-21, 2009

Christopher Wolf,
Editor and Lead Author of the
PLI Privacy and Data Security Law Treatise
Proskauer on Privacy

TABLE OF CONTENTS[*]

[*] Special thanks to Brendon Tavelli for his substantial assistance in the preparation of these materials.

A. The State of Federal Breach Notice and Security Legislation

Despite the widespread adoption, at the state level, of laws that require businesses maintaining personal information to notify individuals when the security of that information may be compromised, efforts to enact comprehensive legislation at the federal level have failed. These efforts appear to be hampered by, among other things, disagreements over the appropriate risk threshold to apply and concerns about displacing relatively strong state laws with a weak, and preemptive, federal law. Efforts to enact comprehensive data security legislation imposing affirmative obligations to protect information similarly have been slow to develop. Still, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (promulgated pursuant to the Gramm-Leach-Bliley Act)[2] and the Health Information Technology for Economic and Clinical Health Act (HITECH), signed into law by President Obama as part of The American Economic Recovery and Reinvestment Act of 2009,[3] create federal data breach notification standards for financial and health data.

1. Introduction

By now, security breach notification laws are fairly common and well-known to privacy professionals. In 2002, legislators across the country began passing laws requiring consumer notification when there is a security breach involving private information. These laws primarily responded to consumer fears of identity theft, heightened by highly publicized data security breaches. As of this writing, forty-three states plus the District of Columbia and Puerto Rico have enacted security breach notification laws affecting private entities.[4] Oklahoma passed a similar law applicable only to

---

[2] 70 Fed. Reg. 15,736 (Mar. 29, 2005).

[3] H.R. 1, 111th Cong. (2009). *See also* Section A.5, *infra.*

[4] Alaska (H.B. 65, tentatively codified at ALASKA STAT. § 45.48.010 *et seq.* and effective July 1, 2009); Arizona (ARIZ. REV. STAT. ANN. § 44-7501); Arkansas (ARK. CODE ANN. § 4-110-101 *et seq.*); California (CAL. CIV. CODE § 1798.82); Colorado (COLO. REV. STAT. § 6-1-716);

state agencies.[5] It is also noteworthy that Georgia's law applies only to information brokers.[6]

Connecticut (CONN. GEN. STAT. § 36a-701b); Delaware (DEL. CODE ANN. tit. 6, § 12B-101 *et seq.*); District of Columbia (D.C. CODE § 28-3851 *et seq.*); Florida (FLA. STAT. § 817.5681); Georgia (GA. CODE ANN. § 10-1-910 *et seq.*) (applies to information brokers only); Hawaii (HAW. REV. STAT. § 487N-1 *et seq.*); Idaho (IDAHO CODE ANN. § 28-51-104 *et seq.*); Illinois (815 ILL. COMP. STAT. 530/1 *et seq.*); Iowa (S.F. 2308, tentatively codified at IOWA CODE § 715C.1 *et seq.*); Indiana (IND. CODE §§ 4-1-11 (state agencies), 24-4.9-1 *et seq.* (all others)); Kansas (KAN. STAT. ANN. § 50-7a01 *et seq.*); Louisiana (LA. REV. STAT. ANN. 51:3071 *et seq.*); Maine (ME. REV. STAT. ANN. tit. 10, § 1346 *et seq.*); Maryland (MD. CODE ANN., COM. LAW § 14-3501 *et seq.*); Massachusetts (MASS. GEN. LAWS ANN. ch. 93H); Michigan (MICH. COMP. LAWS § 445.61 *et seq.*); Minnesota (MINN. STAT. § 325E.61); Montana (MONT. CODE ANN. § 30-14-1701 *et seq.*); Nebraska (NEB. REV. STAT. § 87-801 *et seq.*); Nevada (NEV. REV. STAT. § 603A.010 *et seq.*); New Hampshire (N.H. REV. STAT. ANN. § 359-C:1 *et seq.*); New Jersey (N.J. STAT. ANN. § 56:8-163); New York (N.Y. GEN. BUS. LAW § 899-aa); North Carolina (N.C. GEN. STAT. § 75-65); North Dakota (N.D. CENT. CODE § 51-30-01 *et seq.*); Ohio (OHIO REV. CODE ANN. § 1349.19); Oklahoma (OKLA. STAT. tit. 74, § 3113.1) (applies to state agencies only); Oregon (OR. REV. STAT. § 646A.600 *et seq.*); Pennsylvania (73 PA. CONS. STAT. § 2301 *et seq.*); Puerto Rico (P.R. LAWS ANN. tit. 10, § 4051); Rhode Island (R.I. GEN. LAWS § 11-49.2-1 *et seq.*); South Carolina (S. 453, tentatively codified at S.C. CODE ANN. § 39-1-90 and effective July 1, 2009); Tennessee (TENN. CODE ANN. § 47-18-2107); Texas (TEX. BUS. & COM. CODE ANN. § 48.001 *et seq.*); Utah (UTAH CODE ANN. § 13-44-101 *et seq.*); Vermont (VT. STAT. ANN. tit. 9, § 2430 *et seq.*); Virginia (S.B. 307, tentatively codified at VA. CODE ANN. § 18.2-186.6 and effective July 1, 2008); Washington (WASH. REV. CODE § 19.255.010); Wisconsin (WIS. STAT. § 895.507); West Virginia (S.B. 340, tentatively codified at W. VA. CODE § 46A-2A-101 and effective June 6, 2008); Wyoming (WYO. STAT. ANN. § 40-12-501 *et seq.*). New York City also passed a local security breach notification law, but its provisions were preempted by specific language in the New York state legislation. *See* New York City (Int. No. 141-A, § 20-117); N.Y. GEN. BUS. LAW § 899-aa(9).

[5] OKLA. STAT. tit. 74, § 3113.1.

[6] GA. CODE ANN. § 10-1-911.

Most other U.S. states generally follow California's model breach notification framework in many respects, but also include their own subtle distinctions and provisions governing notification procedures. These distinctions generally relate to when notice to individuals is required, who (besides individuals) must be notified in the event of a breach and how notice is to be provided. Such distinctions are beyond the scope of this article, but the basic provisions of California's framework are introduced below to help understand the many issues in play with respect to enacting a breach notice law at the federal level.

2. The California Framework

The Security Breach Information Act,[7] commonly referred to by its bill number S.B. 1386, was the first law passed in the United States that requires notification to customers for security breaches of personal information. The California law, and most state security breach notification schemes, require notification to individuals after a "breach of the security of the system."[8] A "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information that is maintained by the person or business experiencing the breach.[9] Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not considered a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.[10] A non-owner maintaining data on behalf of an owner must notify the owner of any data security breach immediately upon discovering breach.[11]

---

[7] CAL. CIV. CODE § 1798.82 *et seq.*

[8] *Id.* § 1798.82(a).

[9] *Id.* § 1798.82(d).

[10] *Id.*

[11] *Id.* § 1798.82(b).

Personal information in California is defined as the first name or initial and last name of an individual, with one or more of the following, when either the name or the data elements are not encrypted: Social Security number, driver's license number, credit card or debit card number, a financial account number with information such as PINs, passwords, or authorization codes that could gain access to the account or medical or health insurance information.[12] Publicly available information that is lawfully made available from federal, state, or local government records is not considered personal information.[13]

Subsequent sections of the California Code provide for certain exemptions from the disclosure requirements. One broad exemption is for personal information in encrypted form. Encryption is not defined. Although some might argue that a simple password may qualify for the exemption, the trend is clearly toward more sophisticated protection and the common definition of encryption requires transformation of data into unreadable form. The second is for maintenance of a present interest in a criminal investigation by law enforcement. Other states have developed exemptions for unauthorized access to information from government agencies or entities that are already regulated under federal privacy laws (*e.g.*, FERPA, GLBA, or HIPAA).

---

[12] *Id.* § 1798.82(e). On October 14, 2007, Governor Schwarzenegger approved A.B. 1298 to add medical and health insurance information to the list of personal information elements. "Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. "Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Most other states do not formally recognize medical or health insurance information as "personal information." *But see* ARK. CODE ANN. § 4-110-103(5).

[13] *Id.* § 1798.82(f).

California requires notification in the "most expedient time possible and without unreasonable delay,"[14] either in writing or electronically, if the electronic notice is consistent with federal E-sign standards, which require consumers to consent to the receipt of electronic notice.[15] If a company can show that the cost of notification will exceed $250,000, more than 500,000 people are affected, or the individual's contact information is unknown, then notice may be effected through "substitute notice" consisting of a direct email to the customer, conspicuous posting on a company website, and notification to major statewide media.[16]

3. Federal Pressure Points

Federal legislation, which would likely preempt the patchwork quilt of state laws and create a uniform national standard, has been seriously considered since 2005; however, none has passed as of the date of this writing. The adoption of a uniform national law has been hindered by many factors, including the following:

- the economy as a legislative priority;
- disagreements about when, how and who should be notified in the event of a breach, such as are evidenced by the distinctions among the forty-four plus state security breach notification laws;[17]

---

[14] *Id.* § 1798.82(a).

[15] 15 U.S.C. § 7001.

[16] CAL. CIV. CODE § 1798.82(g). The difference between the electronic notice as primary notice and the email notice as an element of substitute notice is that email notice in conjunction with the other elements of substitute notice does not require consent from the consumer, it is simply a good-faith effort by the entity to notify the individual.

[17] One of the most noted, and perhaps most contentious, developments in security breach notification laws are clauses that require notification only when there is a "material" or "significant" risk of harm from the security breach. At present, the specific requirements establishing a breach as "material" vary by jurisdiction. *Compare* ALASKA STAT. § 45.48.010(c)

- confusion about what congressional committees should exercise jurisdiction over the issue;[18] and

- concerns about whether a single federal law can adequately replace stronger state breach notice laws.

Despite these difficulties, several legislators are expected to make a push for federal breach notice and security laws in the 2009 session. Senator Diane Feinstein (D-Cal.), for example, introduced the "Data Breach Notification Act" (S. 139) on January 6, 2009, the first day of the 111th Congress. The bill, which would preempt conflicting state security breach notification laws, would require businesses and federal agencies to notify individuals if the security, confidentiality or integrity of their sensitive personal information is compromised. In addition, Rep. Rick Boucher (D-Va.) has expressed an interest in pursuing data privacy legislation in his new role as chairman of the House Subcommittee on

---

(notification is not required if after an appropriate investigation and written notification to Alaska's attorney general, the covered person determines that there is not a reasonable likelihood that harm to consumers will result from the breach) *with* MICH. COMP. LAWS § 445.72 (notification required "unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to [one] or more residents").

The continuing debate over the proper risk of harm threshold is a significant obstacle to the adoption of a federal breach notification law. Certain consumer advocates have voiced concern with the "material harm" standard as a trigger for notification, arguing this standard creates too high a bar for notification. Furthermore, they contend that without meaningful guidance about the terms "reasonable investigation," "significant risk," and similar language in the laws, the terms are open to such wide interpretation that they may become meaningless and provide no protection. However, others counter that there will be unnecessary over-notification without such a trigger. This may result in customers becoming desensitized to notification and failing to take the appropriate steps to protect themselves from identity theft when a data security breach takes place that creates an actual risk of harm.

[18] Over the past several years, at least six federal legislative committees have claimed some ownership over data security legislation issues.

Communications, Technology, and the Internet ("CTI Subcommittee"). The precise contours of Boucher's proposal are still being finalized as of this writing, but Boucher hopes to work with Rep. Cliff Stearns (R-Fla.) – the ranking Republican on the committee – to develop at least some aspects of the legislation. Rep. Edward Markey (D-Mass.), whom Boucher is replacing as Chairman of the CTI Subcommittee, is also rumored to be considering the introduction of a privacy bill. The details of Markey's proposal, however, are still unclear.

4. Interagency Guidance on Response Programs

On March 29, 2005, a group of financial institution regulators comprised of the Comptroller of Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision released its Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("Interagency Guidance").[19] The Interagency Guidance requires financial institutions to develop and implement a security response program to address incidents of unauthorized access or use of customer information. A data breach response plan generally includes not only notice to consumers but also the following components: (1) assessing the situation; (2) notifying regulatory and law enforcement agencies; (3) containing and controlling the situation; and (4) taking corrective measures.

The response plan requirement is limited to sensitive customer information, which, if compromised, *may cause substantial harm or inconvenience to the consumer*. This includes a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, or other account information and PIN numbers.

---

[19] 70 Fed. Reg. 15,736 (Mar. 29, 2005). *See also* 12 C.F.R. pt. 30, app. B, Supplement A (OCC); 12 C.F.R. pt. 208, app. D-2, Supplement A and 12 C.F.R. pt. 225, app. F, Supplement A (Federal Reserve Board); 12 C.F.R. pt. 364, app. B, Supplement A (FDIC); 12 C.F.R. pt. 570, app. B, Supplement A (OTS).

Most importantly, the response plan requirement is flexible. The agencies realized that not all financial institutions are alike in their operations. Thus, imposing upon a local bank (with only one or a couple branch offices) the same requirements as may be necessary or desirable with respect to a nationwide banking institution would be unfair. So the agencies adopted a flexible standard. Under the Guidelines, financial institutions may tailor their security response programs to their size, complexity, and the nature of their operations. But a regulated institution's response program should contain procedures for the following, at a minimum:

- Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;

- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of "sensitive" customer information;

- Consistent with the agencies' Suspicious Activity Report (SAR) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and,

- Notifying customers when warranted.[20]

Regulated entities that are subject to the Interagency Guidance may therefore be obligated to provide notice of an information security breach in some cases.

---

[20] *Id.*

5. HITECH Notification Obligations

On February 17, 2009, data breach notice provisions applicable to health information were signed into law as part of the HITECH Act provisions of the massive economic stimulus legislation, H.R. 1.[21] Beginning no later than September 16, 2009,[22] "covered entities" under the Health Insurance Portability and Accountability Act ("HIPAA")[23] will be required to give notice of breaches in the security of protected health information, and "business associates" of such entities will be required to report such breaches to the covered entities. The breach notice provisions apply to protected health information ("PHI") that is "unsecured."[24] Section 13402(a) of the HITECH Act provides that a "covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall notify each individual whose information has been subject to a breach."

---

[21] H.R. 1, 111th Cong. (2009).

[22] The effective date of the breach notification provisions depends upon when the Secretary of HHS issues implementing regulations. The legislation directs the Secretary to issue interim final regulations within 180 days of enactment of the legislation, the breach notice provisions become effective 30 days following the issuance of the regulations and apply to breaches discovered on or after that date. Under that scheme the effective date should be no later than September 16, 2009.

[23] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[24] The term "unsecured" is to be addressed in regulations issued by the Secretary of Health and Human Services no later than August 17, 2009. However, the legislation goes on to define the term in the event that the required regulations are not timely issued. The "backstop" definition of PHI that is "not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute."

5.1. What is a "breach"?

The term "breach" is defined as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."

In addition to the exception language in the above portion of the definition, there is a further exception for certain circumstances involving inadvertent acquisition, access or use of PHI by employees and agents of covered entities or business associates where the information is not further acquired, accessed, used or disclosed. §13400(1)(B)

5.2. Timing and nature of notification

Notice of a breach must be given "without unreasonable delay" and in no event later than 60 days after the date of discovery of the breach. §13402(d). Notice must be given to the individual whose PHI was subject to a breach, or to the next of kin in the case of a deceased person, to the last known address of the person or the next of kin. E-mail notice may be given only if the individual specified e-mail notice "as a preference."

If the contact information of an individual is insufficient or out of date, "a substitute form of notice" must be provided; if the information is insufficient or out of date for 10 or more persons, such substitute notice must be given in the media and on the Web site of the covered entity, as further provided in the Act and under regulations to be adopted by the Secretary of HHS. In a case in which "urgency" is required "because of possible imminent misuse" of unsecured PHI, the covered entity may provide notice "by telephone or other means, as appropriate."

If the breach involves unsecured PHI of 500 or more individuals, both media notice and notice to the Secretary of HHS must be given. Covered entities must also report to the Secretary of HHS on an annual basis as to any breaches that have occurred, even if reporting to the Secretary was not otherwise required (i.e., the

breach involved the unsecured PHI of less than 500 individuals). §13402(e)(3).

Like most state data security breach notification statutes, there is an exception to the timing requirement if a delay is requested by law enforcement officials.

5.3. Application to "business associates"

The notice provisions require a "business associate" (as such term is defined in the administrative simplification regulations promulgated under HIPAA)[25] that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses" unsecured PHI of a covered entity to notify the covered entity in the event of a breach in the security of such information. The notice must include, among other things, "the identification of each individual whose unsecured protected health information" was breached.

Although the HIPAA Privacy Rule and Security Rule currently mandate that covered entities include in their contracts with business associates provisions requiring that the business associate notify the covered entities of: a) uses and disclosures of protected information not provided for by its contract, and b) "security incidents" (as defined in the HIPAA Security Rule), the new law now directly imposes notification obligations on the business associate. Because the obligation on business associates to report such breaches to covered entities will now be statutory, failure to comply will be more than just a breach of contract – now business associates could be subject to civil and criminal penalties.

[25] Business associates are persons or entities who provide certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of PHI. Examples of business associate functions include claims processing or administration, quality assurance, billing, benefit management, and practice management as well as legal, actuarial, accounting, consulting, administrative, or financial services.

5.4. Application to "vendors of personal health records"

Section 13407 contains a separate set of "temporary"[26] breach notification provisions that target enterprises that offer services to individuals to store their health information online as well as their service providers. The provisions reflect concerns that such vendors are not subject to the HIPAA Privacy Rule, even as the Medicare program itself is implementing programs to encourage beneficiaries to use such private services to maintain their personal health records.

A "vendor of personal health records" is defined in § 13400(18) as "an entity, other than a covered entity [under HIPAA], that offers or maintains a personal health record." Such vendors, as well as a list of other entities involved in providing various services related to personal health records, are generally required to provide notice of a breach in the security of identifiable health information that is (1) provided by or on behalf of the individual and that (2) identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

The notice must be provided to the affected individuals, as well as to the Federal Trade Commission. Violations of the data security breach provisions are defined as an unfair or deceptive act or practice under the FTC Act, and the FTC is tasked with adopting regulations and enforcing the provisions of this section.

5.5. Preemption

With respect to preemption of state law, the HITECH Act references the provisions in the Social Security Act that set forth the general rule preempting contrary state laws, but *excepting* from that general rule a state law that "relates to the privacy of

[26] These provisions are designated as temporary because they will lapse in the event that Congress enacts new data security breach legislation applicable to non-HIPAA entities. § 13407(g).

individually identifiable health information."[27] The HITECH Act data breach provisions themselves are contained in Subtitle D – "Privacy" of the Act and the legislative history is replete with references to the provisions as protective of patient privacy, so state data security breach laws that apply to health information "relate to the privacy of health information." Therefore, to the extent that a state security breach law similarly pertains to health information and is more protective of such information than the new federal provisions, it would appear not to be preempted by the security breach provisions in the HITECH Act, and business associates and covered entities, to the extent that they are covered by both federal and state laws, would be required to comply with both laws.

B. Federal Efforts in Electronic Healthcare Records and Systems

Many believe that digitizing patient records has the capacity to dramatically transform the delivery of medical services in the United States. As a result, the transition from paper to electronic health records ("e-health records") has been considered and discussed extensively by federal government officials. For example, through the Department of Health and Human Services Electronic Health Records Workgroup ("EHRW"),[28] the federal government has been considering the logistics of implementing a federal e-health records management system for several years. And in 2004, then-President George W. Bush issued an Executive Order establishing the position of the National Coordinator for Health Information Technology within the Office of the Secretary of Health and Human Services ("HHS"), the primary purpose of which was to aid the Secretary of HHS in achieving the President's goal for most Americans to have access to an interoperable electronic medical record by 2014.

---

[27] § 13421(a).

[28] The EHRW's task is to "To make recommendations to the Community on ways to achieve widespread adoption of certified [e-health records], minimizing gaps in adoption among providers." *See* Electronic Health Records Workgroup, http://www.hhs.gov/healthit/ahic/healthrecords.

The issue of e-health records, however, took on renewed prominence during the 2008 presidential election campaign because e-health records are an integral part of now-President Barack Obama's plan to reduce healthcare costs in the United States. Even more recently, with the passage of the economic stimulus bill that designates approximately $19 billion for healthcare IT spending, the fervor surrounding such records rose to new and greater heights. The digitization of patient records increases the importance of attention to privacy and data security, especially in light of the enhanced HIPAA rules.[29]

1. Ongoing Federal efforts

Despite the widely-shared belief that the adoption of e-health record systems will greatly benefit the U.S. healthcare system, such systems are not common outside of the Veterans Health Administration system. This is something the Bush administration sought to change, even before Senator John McCain and then-Senator Barack Obama drew the nation's attention to the potential benefits of digitizing patient records during the 2008 campaign. Most of the progress made by the previous administration, however, involved forming working groups to consider relevant e-health record issues, appointing personnel to lead the charge and sketching out the foundations of, and recommendations for, an effective e-health records system.

Some Congressional leaders also have attempted to take proactive steps toward the adoption of e-health record systems. In 2008, members of the Senate and the House introduced legislation aimed at fostering the development of e-health record systems. The adoption of such systems, however, is severely hampered by concerns about the following:

- **start up costs:** implementing e-health record systems cost money that many smaller practices do not have, or do not want to spend on an unproven commodity

[29] *See supra* text accompanying notes 21-23.

- **transition lags:** training personnel on new systems likely means that patients and providers will experience short-term service disruptions

- **poor standardization:** to be effective, terminology and technology should be standardized across providers and systems

- **interoperability and synchronization:** to be valuable, systems must be able to easily communicate with one another and update "simultaneously"

- **fear of change:** many providers are resistant to adopting new systems and business practices

- **privacy risks:** many providers and individuals fear that e-health records are less secure than paper records, and health information may be easily compromised

- **maintenance costs:** providers will likely need to invest considerably in IT spending required to keep systems up-to-date, and IT failures could be costly

As a result of these, and other concerns, we have seen little concrete progress toward the roll-out of a federal e-health records system. But it is clear that the new administration intends to focus extensively on making improvements in this area.

2. Stimulus Funding for e-health records

As planned, the passage of The American Economic Recovery and Reinvestment Act of 2009[30] has doctors and information technology specialists scrambling to prepare for the availability of approximately $19 billion in funds dedicated to healthcare IT. The vast majority of these funds, approximately $17 billion, will be distributed in the form of Medicare and Medicaid reimbursements, to practitioners that implement and use e-health record systems. The remaining $2 billion is earmarked to aid the development of

[30] H.R. 1, 111th Cong. (2009).

adequate industry standards and training programs for the personnel needed to operate such systems.

The incentive payments are intended to approximate the per-physician cost to implement an appropriate e-health record system. Under the stimulus package, healthcare providers that meet certain implementation standards and benchmarks will receive five annual payments of $18,000, $12,000, $8,000, $4,000 and $2,000 between now and 2014. These implementation standards include using a system with the ability to share information with other healthcare providers.

After 2014, no incentives will be offered to those who are meaningfully using e-health record systems. Rather, providers without such systems in place will be penalized. Beginning in 2014, healthcare providers that still do not have an approved e-health record system in place will see their Medicare reimbursements progressively reduced.

President Obama, and those involved in passing the stimulus bill, hope that the bill's carrot and stick scheme will both ease the financial burden on physicians and hospitals that digitize patient medical records and spur the rapid adoption of e-health record systems.

C. Implementation of the Red Flags Rules

1. Introduction

New regulations promulgated by the Federal Trade Commission ("FTC") and the federal banking agencies require covered companies that hold any customer accounts to implement identity theft prevention programs that identify and detect "Red Flags" signaling possible identity theft. Under these regulations, companies establishing such programs must create policies and procedures not only to recognize and detect Red Flags, but also to respond to Red Flags by preventing or mitigating potential identity theft. Furthermore, companies must develop reasonable policies and procedures to verify the identity of a customer opening an account, and must also periodically update their identity theft programs. The rules went into effect on January 1, 2008. As will

be described in more detail below, compliance with the rules was required by November 1, 2008 for businesses regulated by the federal banking agencies and by May 1, 2009 for FTC-regulated entities.[31]

1.1. Scope of the Red Flags Rule

Federal regulators issued the final Red Flags rules pursuant to Section 114 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which requires these agencies to identify patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft. The final rules apply to all financial institutions and creditors that hold or maintain "covered accounts" defined as "(1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft." Under the rules, financial institutions are defined in accordance with the Fair Credit Reporting Act and include banks, mortgage lenders, savings and loan associations, mutual savings banks, credit unions or any other person that, directly or indirectly, holds a transaction account belonging to a consumer. Creditors are defined as persons or businesses that arrange for the extension, renewal, or continuation of credit," and thus encompass a wide range of entities, including car dealers, utilities, as well as third-party debt collectors.

Given the broad reach of the regulations, the agencies gave financial institutions and creditors significant flexibility to determine which Red Flags are relevant to detect identity theft. According to the final rules, businesses "may tailor the Red Flags it chooses for its Program to its own operations. A financial institution or creditor will not need to justify to an Agency its failure to include in the Program a specific Red Flag from the list of examples. However, a covered entity will have to account for

[31] For more details, see *A Practical Guide to the Red Flag Rules: Identifying and Addressing Identity Theft Risks* (Christopher Wolf & Kristen J. Mathews, eds., Practising Law Institute 2008).

the overall effectiveness of a Program that is appropriate to its size and complexity and the nature and scope of its activities." Additionally, the rules suggest that companies acquire approval of the program from the board of directors or a committee of the board, as well as exercise oversight of the implementation of the program, training staff and employees, and service provider arrangements.

1.2. Examples of Red Flags

To assist financial institutions and creditors in choosing which Red Flags to identify, the agencies provide an extensive list of possible Red Flags that may require further action when they come to the attention of a company, consisting, in part, of the following:

- A fraud alert, credit freeze, or address discrepancy is included with a consumer report or provided by a credit reporting agency.

- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer.

- Documents, applications, or photo identification provided appear to have been altered or forged, or give the appearance of having been destroyed and reassembled.

- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

- Personal identifying information provided is inconsistent when compared to other personal identifying information on file with the financial institution or creditor or provided by the customer (i.e., there is a lack of correlation between the SSN range and date of birth), or otherwise inconsistent when compared against external information sources used by the financial institution or creditor.

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor.

- The SSN, address or telephone provided is the same as that submitted by other customers or by an unusually large number of other persons opening accounts.

- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

- A covered account is used in a manner that is not consistent with established patterns of activity on the account.

As stated above, businesses must also implement customer verification procedures. Financial institutions subject to the existing Customer Identification Program ("CIP") rules promulgated under Section 326 of the USA PATRIOT Act may satisfy the FACTA customer verification procedures by complying with CIP. Nevertheless, "[t]he Agencies expect all financial institutions and creditors to evaluate the adequacy of existing policies and procedures and to develop and implement risk-based policies and procedures that detect Red Flags in an effective and comprehensive manner."

1.3. FDIC and Federal Reserve guidance

As of October 2008, both the Office of Thrift Supervision ("OTS")[32] and the Federal Reserve Board ("Federal Reserve")[33] had issued their instructions for examiners on enforcement of the new Red Flags rule. These instructions are used by examiners to evaluate whether regulated entities are in compliance with the rules. The instructions require examiners to, among other things, request internal reports related to a company's identity theft red flag program and documents pertaining to incidents of identity theft and the associated response(s) by the covered entity. The OTS and Federal Reserve examiner instructions, however, otherwise closely track the language and structure of the Red Flags rules. Consequently, they offer very little guidance to companies as they take steps to comply.

2. Compliance extension from the FTC

The FTC announced in October 2008 that it would not enforce the new Red Flags rules until May 1, 2009, giving financial institutions and creditors an additional six months to comply by developing and implementing a written identity theft prevention program. In an Enforcement Policy Statement released on October 22, 2008, the FTC acknowledged the uncertainty felt by many entities and some industries regarding whether they would be considered "covered entities" and thus subject to the rules. The FTC's announcement, however, did not affect companies subject to the enforcement authority of federal agencies other than the FTC.

---

[32] Office of Thrift Supervision, *Information Technology Risks and Controls and Fair Credit Reporting Act* (Oct. 24, 2008), *available at* http://files.ots.treas.gov/74843.pdf.

[33] Federal Reserve, *Interagency Examination Procedures: Section 615(e) Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft (12 CFR 222.90)*, http://www.federalreserve.gov/boarddocs/srletters/2008/SR0807a2.pdf.

2.1. Confusion Among Companies Regarding Coverage

The rules apply to financial institutions and creditors. But according to the FTC, many companies "indicated that they were not aware that they were engaged in activities that would cause them to fall under the FACT Act's definition of creditor or financial institution." Moreover, the FTC said that companies not traditionally subject to the jurisdiction of the FTC did not follow the FTC's rulemaking, and consequently did not become aware of their obligations under the Red Flags rules until too late. The FTC also expressed concern that covered entities, to meet the fast approaching November 1 deadline, were not taking the appropriate care necessary to do a proper risk assessment and craft a meaningful red flag program.

As the FTC stated, "[g]iven the confusion and uncertainty within major industries under the FTC's jurisdiction about the applicability of the rule, and the fact that there is no longer sufficient time for members of those industries to develop their programs and meet the November 1 compliance date, the Commission believes that immediate enforcement of the rule on November 1 would be neither equitable for the covered entities nor beneficial for the public." Therefore, the FTC delayed enforcement of the new rules for six months.

2.2. Clarification as to who and what is covered

In the wake of the FTC's extension, a company must carefully consider whether it would be considered a covered entity – i.e., a financial institution or a creditor. Financial institutions include banks, mortgage lenders, savings and loan associations, mutual savings banks, credit unions or any other person that, directly or indirectly, holds a transaction account belonging to a consumer. As to the definition of creditor, the Red Flags rules reference the Equal Credit Opportunity Act ("ECOA"), which defines a creditor as anyone who grants to a debtor the right "to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor." In its Enforcement Policy Statement, the FTC noted that under the ECOA's definition, "any person that provides a product or service for which the consumer pays after delivery is a creditor." Thus, under this broad

interpretation, many companies that permit their customers to defer payment for any purchase may be covered under the rules.[34]

Once a company determines that it is indeed a covered entity, it must assess which of its accounts or products fall under the definition of "covered accounts" – a red flag program need only apply to these covered accounts. The definition of "covered account" is divided into two parts: (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.

Covered entities then must develop written policies and procedures not only to identify and detect red flags, but also to respond to red flags by preventing or mitigating potential identity theft. Because covered entities must tailor their red flags programs to their particular business, these companies will need to do risk assessment to evaluate current identity theft prevention measures, their shortcomings and the risks to customers. In addition, companies must periodically update their identity theft programs to address emerging threats.

3. Tracking compliance with the Red Flag Rules

While it is still fairly early to evaluate the level of compliance with the new Red Flags rules, initial reports suggest that it will be difficult and expensive for many companies to comply by the relevant deadlines. For example, a survey conducted by Compliance Coach Inc., which advises creditors with respect to regulatory compliance, revealed that approximately 91 percent of hospitals expected to spend up to $10,000 to achieve compliance, and the remaining 9 percent expected to spend up to $50,000. Nonetheless, it is important for businesses to take steps to comply within the relevant timeframes.

---

[34] The broad reach of the new rules likely encompasses hospitals, among other entities not traditionally subject to the FTC's jurisdiction, many of which often allow patients to defer payment for services.

The Federal Deposit Insurance Corporation ("FDIC"), the Office of Thrift Supervision ("OTS") and other banking agencies planned to begin enforcing the new rules as of the November 1, 2008 compliance deadline. Regulators within these organizations believe that sufficient outreach was conducted in advance of the implementation of the new rules such that the regulated community understands the need to be in compliance by that date. These regulators, however, indicated that the imposition of civil penalties for noncompliance during the initial phase of enforcement would be extremely unusual.

The FTC too, in light of the six-month extension announced in October 2008, will likely begin enforcing the new Red Flags rules immediately after the May 1, 2009 compliance deadline.

D. Update on REAL ID

Signed in 2005, the federal REAL ID Act enshrines into law certain authentication, issuance and security standards for state driver's licenses and other state ID cards. Under REAL ID, only ID cards that meet these standards will be accepted for "official purposes," as defined by the Secretary of the Department of Homeland Security ("DHS").[35] But the development of a national identification system, such as that mandated by REAL ID, clashes with the United States' historical reluctance to allow the federal government to issue, and demand, uniform identification cards. Moreover, the implementation of a nationwide identification system raises serious privacy concerns related to protecting the personal information that must be collected and stored as a necessary corollary to issuing such identification cards. Consequently, since its enactment, REAL ID has encountered staunch resistance from states and consumer advocates.

[35] "Official purposes" include boarding commercial airline flights, entering federal buildings that require identification and entering nuclear power plants.

1. State refusal to comply with REAL ID

Since 2005, more than a dozen states have passed legislation prohibiting the implementation of REAL ID. And other states, including Missouri,[36] will consider similar legislation during the 2009 session. States have rejected the implementation of REAL ID for a variety of reasons, including the potentially enormous expense required to develop a compliant program. It is estimated that implementing REAL ID will cost states more than $11 billion over five years. According to the National Governors Association ("NGA"), the requirement for states to implement a REAL ID compliant program constitutes an unfunded federal mandate that states cannot afford.[37] Moreover, the NGA and others believe that the timelines and requirements mandated by REAL ID are unrealistic. Consequently, as of this writing, only a handful of states have taken steps to upgrade their identification systems to meet objectives similar to those of REAL ID.[38] One such state, Washington, took steps toward compliance largely as an alternative to the DHS's Western Hemisphere Travel Initiative ("WHTI").[39] Washington state's security-enhanced driver's licenses, which require proof of citizenship, identity and residence and include passport-like security features, are accepted for purposes of crossing into the state from Canada.

---

[36] *See* Alyson E. Raletz, *Guest Warns Against Big Brother, Real ID*, stjoenews.net (Feb. 11, 2009).

[37] *See, e.g.*, Letter to DHS Secretary Michael Chertoff from Governors Huckabee and Napolitano (Oct. 6, 2005), *available at* http://www.nga.org.

[38] Notably, if certain compliance benchmarks are demonstrated in timely fashion, the final rule allows states to obtain extensions until December 1, 2014 to fully comply with REAL ID requirements for driver's licenses for individuals born after Dec. 1, 1964, and until Dec. 1, 2017, to comply for individuals born on or before Dec. 1, 1964.

[39] Set in motion in January 2008, the WHTI required U.S. citizens to present a passport when they re-entered the country from Canada, Mexico or Bermuda.

2. Compliance obstacles

In addition to REAL ID's significant financial burdens, the Act also presents certain administrative challenges for the states required to implement its mandates.

2.1. Privacy protections

Foremost among these challenges is the difficulty of protecting the tremendous amount of sensitive personal information collected and stored pursuant to a REAL ID compliant program, both on individual identification cards and in centralized databases. Privacy advocates are concerned that a robust legal framework of U.S. privacy laws does not exist to protect personal information in a centralized identification database, such as that being considered in conjunction with the Act's implementation. Moreover, privacy advocates want to be sure that any personal information stored in the bar code for REAL ID compliant identification cards is adequately protected from misuse. The DHS's proposed rule[40] implementing REAL ID included tamper proof card design standards. However, DHS removed these design requirements from its final rule implementing REAL ID,[41] and rejected proposals to require encryption of such information, because such requirements conflicted with law enforcement's need for quick and easy access to the information. Privacy advocates fear that not encrypting the bar code will help push the REAL ID system into widespread use, beyond the enumerated federal purposes for which it is designed.

2.2. Burden on state DMV officials

Another concern expressed by opponents of REAL ID is the potential strain on state Department of Motor Vehicles ("DMV")

---

[40] Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Notice of Proposed Rulemaking, 72 Fed. Reg. 10,820 (Mar. 9, 2007).

[41] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule, 73 Fed. Reg. 5,271 (Jan. 29, 2008) (to be codified at 6 C.F.R. pt. 37).

personnel. Under REAL ID, state DMV staff are required to verify the authenticity of source documents before issuing REAL ID compliant identification cards. These source documents include a photo identity document and documents that establish the person's date of birth, Social Security number, name, address, principal residence and lawful status. However, some argue that it is not clear that state DMV personnel will be able to effectively recognize fraudulent documents even after receiving appropriate training, and that the final rules fail to specify what recourse exists if it is determined that source documents are fraudulent.[42] In addition, there is concern that some U.S. citizens will not be able to produce the types of source documents called for in the final REAL ID regulations. For these reasons, among others, the REAL ID program is fraught with potential for error with respect to the issuance or denial of enhanced identification cards.

3. DHS Secretary opposed REAL ID

The appointment of Janet Napolitano as the Secretary of the Department of Homeland Security offers a ray of hope to those states, and others, that oppose REAL ID. While acknowledging the importance of secure and effective identification mechanisms, Secretary Napolitano has openly questioned the propriety of REAL ID as a vehicle for achieving this objective. During her term as governor of Arizona, Secretary Napolitano signed a bill opting the state out of REAL ID until the federal government committed to pay the costs associated with developing and implementing the national ID system. Secretary Napolitano intends to create a working group of governors to assess the costs and benefits of secure identification methods, and to evaluate "realistic" alternatives.

In addition to Secretary Napolitano's own open criticisms of REAL ID, the DHS Data Privacy and Integrity Advisory Committee recently submitted a letter to Napolitano and Acting DHS Chief Privacy Officer, John W. Kropf, which stated that "the

---

[42] *See, e.g.*, REAL ID Implementation Review: Few Benefits, Staggering Costs, EPIC (May 2008), *available at* http://epic.org/privacy/id-cards/epic_realid_0508.pdf.

final rule under the REAL ID Act does not fully address privacy and data security."[43] The Committee further stated that the final rule not only "leaves states in the position of subjecting their residents' personal information to the vulnerabilities of the state with the weakest protections," but also "encourages inappropriate data collection and mission creep."[44] Thus, the Committee suggested that REAL ID be reviewed and considered for revision, particularly since the final rule has not yet gone into full effect.

Though it is too early to tell what steps DHS will take with respect to implementing REAL ID, it seems likely that the Department will march in a different direction under new leadership.

E. Recent Actions and Guidance from Gramm-Leach-Bliley Regulators

The Gramm-Leach-Bliley Act ("GLBA")[45] applies to "financial institutions," which includes businesses "significantly engaged in providing financial services to consumers." But the GLBA's requirements are used by plaintiffs' attorneys and state and federal law enforcement and regulatory agencies as a touchstone for what is "reasonable" with respect to the protection of personally identifiable information ("PII"). The process-oriented focus of GLBA enforcement agencies has resulted in guidance on what steps a business can take to be effective and "reasonable" in protecting consumer privacy.

1. Introduction

The Federal Trade Commission ("FTC"), one of the principal agencies charged with enforcement of the GLBA, has enacted two major rules under the GLBA: (1) the Privacy Rule and (2) the Safeguards Rule.

---

[43] Letter from J. Howard Beales to Janet Napolitano & John W. Kropf (Feb. 3, 2009), *available at* http://techdailydose.nationaljournal.com.

[44] *Id.*

[45] 15 U.S.C. § 6801 *et seq.*

1.1. Privacy Rule

The Privacy Rule sets forth disclosures that must be made to consumers, including 1) the categories of nonpublic personal information collected and/or disclosed, 2) the affiliates and the nonaffiliated third parties to whom such information is disclosed, and 3) a description of the customer's right to prevent certain disclosures.[46] It also contains limits on use and disclosure of non-public personal information.

1.2. Safeguards Rule

The Safeguards Rule requires institutions to adopt a comprehensive information security program for protecting consumers' nonpublic personal information. The program must be in writing and must contain "administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature of your activities, and the sensitivity of any customer information at issue."[47]

Implementing a Safeguards Rule compliant program does not involve specific mandates. Instead, it is a process-oriented approach that should involve:

- conducting a risk assessment to evaluate physical, technical and individual risks;
- appointing a single employee, preferably one with a legal background, to oversee privacy and data security;
- testing and monitoring relevant safeguards and making revisions when necessary to ensure the protection of nonpublic personal information;
- creating a data breach response plan;

[46] *See* 16 C.F.R. § 313.4 *et seq.*

[47] 16 C.F.R. § 314.3.

- overseeing vendors that use or access sensitive data; and

- implementing policies for disposal of records that are no longer needed.

2. Guidance from GLBA regulators

In 2008, the contours of the GLBA continued to be refined more through enforcement, which will be described below, than through affirmative pronouncements by the GLBA regulators. One area in which many expected to see activity relates to the development of a model GLBA privacy notice.[48]

In an effort to make required GLBA privacy notices more comprehensible to consumers, on March 21, 2007, eight federal regulatory agencies ("Joint Agencies") with jurisdiction over GLBA regulated "financial institutions" issued an interagency proposal for a new model privacy form. The model form was largely based on a report issued by the Kleimann Communications Group in March 2006. The proposed model form includes 2-3 pages, depending on whether there is an opt-out; general background information and a keyframe with why, what and how information regarding a financial institution's use of personal information, reasons for sharing, and opt-out rights; and supplementary information such as definitions and further explanatory information in the form of Frequently Asked Questions. The proposed rules require a minimum font size and that financial institutions provide sufficient spacing between lines

[48] Section 503 of the GLBA and current rules, require financial institutions to provide their customers with a notice that describes, among other things, how they protect nonpublic personal information, the categories of nonpublic personal information collected, the affiliates and the nonaffiliated third parties to whom such information is disclosed, and a description of the customer's right to prevent certain disclosures to nonaffiliated third parties. These notices must be provided at the outset of the institution's relationship with a customer and, in the case of long-standing relationships, on an annual basis. Current rules do not mandate a standard format or particular wording for the notices, however, they provide sample clauses that financial institutions can use to satisfy the notice requirements.

of type with further recommendations on font type, spacing, paper size and color.

As of this writing, contrary to predictions by those close to the issue that a model form would issue by the end of 2008, the interagency model form is still a work in progress. Similarly, despite the issuance of proposed amendments to Regulation S-P in March 2008, the U.S. Securities and Exchange Commission's efforts to amend its existing privacy rules mandated under the GLBA continue to evolve.

3. GLBA enforcement

Pursuant to its Privacy and Safeguards Rules, the FTC continues to actively pursue companies that mislead consumers about their information security practices and/or fail to adequately protect personal information. In 2008, the FTC announced two settlements, with Goal Financial LLC and Premier Capital Lending, Inc., related to violations of the Privacy and Safeguards Rules.

3.1. Goal Financial

The FTC's administrative proceeding against Goal Financial LLC[49] alleged that the company both failed to adequately protect personal information it collected and failed to live up to promises it made in its online privacy policy. According to the FTC's complaint, Goal Financial allowed more than 7,000 files containing personal information to reach third parties without proper authorization. The FTC further alleged that a Goal Financial employee improperly sold surplus hard drives containing information about approximately 34,000 consumers. On April 9, 2008, the Commission approved a final consent decree that requires the company to implement a comprehensive information security program and obtain independent security audits every other year for ten years. The consent decree also prohibits further misrepresentations regarding the company's security practices.

[49] *In re Goal Financial LLC*, FTC, No. 072-3013, http://www.ftc.gov/os/caselist/0723013/index.shtm.

3.2. Premier Capital

On November 6, 2008, the FTC announced a settlement with Premier Capital Lending, Inc., a Texas-based mortgage lender.[50] In its complaint, the FTC accused Premier of making customer information vulnerable by allowing a third-party home seller to use a Premier account to access consumer reports without taking steps to verify the seller's practices with respect to handling, storing and disposing of sensitive personal information. The FTC alleged that this practice violated the Safeguards Rule. The FTC further alleged that Premier violated the Privacy Rule by failing to live up to the promises it made in its online privacy policy, which, among other things, provided that "[o]ur control policies . . . authorize access to customer information only by individuals who need access to do their work."

If approved, Premier's settlement with the Commission will require the company to implement a comprehensive data security program, obtain independent audits of the program on a biennial basis for twenty years, and maintain a copy of each document related to compliance with the terms of the settlement.

F. FTC Self-Regulatory Principles for Online Behavioral Advertising

On February 12, 2009, the FTC issued its long-anticipated Staff Report on Self-Regulatory Principles for Online Behavioral Advertising.[51] The revised Self-Regulatory Principles are the result of a year of study of the more than sixty comments provided by industry, advocacy organizations, academics, and individual consumers in response to the FTC's proposed self-regulatory principles issued in late 2007.

---

[50] *In re Premier Capital Lending, Inc.*, FTC File No. 072-3004 (2008), http://www.ftc.gov/os/caselist/0723004/index.shtm.

[51] Federal Trade Commission, FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (hereinafter "FTC Staff Report").

Not surprisingly, the FTC made clear that "these Principles are guidelines for self-regulation and do not affect the obligation of any company (whether or not covered by the Principles) to comply with all applicable federal and state laws."[52] And the Principles themselves, set forth below, largely reflect existing FTC law in this area. For example, it is well established that a company may not unilaterally alter its policies and use previously collected data in a manner that materially differs from the terms under which the data was originally collected.[53]

The FTC defines online behavioral advertising as "the tracking of a consumer's online activities over time – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests." The newly revised Principles now explicitly carve out "first party" advertising, where no data is shared with third parties, and contextual advertising, where an ad is based on a single visit to a web page or single search query.

The Report notes the eroding distinction between traditional personal identifying information ("PII") such as name, address and Social Security number, and non-PII such as IP address. As set forth in the Executive Summary, the "staff believes that the Principles should apply to data that could reasonably be associated with a particular consumer or computer or other device, regardless of whether the data is 'personally identifiable' in the traditional sense. In the context of online behavioral advertising, rapidly changing technologies and other factors have made the line between personally identifiable and non-personally identifiable information increasingly unclear. Moreover, this approach is consistent with existing self-regulatory efforts in this area."[54]

---

[52] *Id.* at 45.

[53] *See In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004).

[54] FTC Staff Report, *supra* note 49, at ii-iii.

Those blurring lines and increasingly complex technology and advertising practices promise to pose considerable challenges for the construction of clear and user-friendly consumer privacy notices.

The Report makes clear that disclosures regarding the collection of PII and non-PII for purposes of behavioral marketing should be made *separate* from the traditional privacy policy. "Staff recognizes that it is now customary to include most privacy disclosures in a website's privacy policy. Unfortunately, as noted by many of the commenters and by many participants at the FTC's November 2007 Town Hall, privacy policies have become long and difficult to understand, and may not be an effective way to communicate information to consumers. Staff therefore encourages companies to design innovative ways – outside of the privacy policy – to provide behavioral advertising disclosures and choice options to consumers." The Staff Report highlights certain recommendations made by commenters that "appear promising. For example, a disclosure (e.g., 'why did I get this ad?') that is located in close proximity to an advertisement and links to the pertinent section of a privacy policy explaining how data is collected for purposes of delivering targeted advertising, could be an effective way to communicate with consumers. . . . Staff encourages these efforts and notes that they may be most effective if combined with consumer education programs that explain not only what information is collected from consumers and how it is used, but also the tradeoffs involved – that is, what consumers obtain in exchange for allowing the collection and use of their personal information."

The Principles provide for: (1) transparency and consumer control; (2) reasonable security, and limited data retention, for consumer data; (3) affirmative express consent for material changes to existing privacy promises; and (4) affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising.

G. Deferral of E-Verify Regulations

Enforcement of a controversial federal regulation that raised significant privacy concerns has been postponed once again as the

result of a legal challenge filed by the Chamber of Commerce of the United States of America and four other trade associations. *See Chamber of Commerce of the U.S. v. Napolitano*, Civil Action No. AW-08-3444 (D. Md.). The regulation in question would have required most government contractors and subcontractors to participate in E-Verify, an Internet-based system that allows employers to verify that individuals are eligible to work in the United States using an employee's Social Security number and other personal information. Pursuant to a January 27, 2009 agreement between the parties, enforcement of the regulation has been postponed until May 21, 2009, in order to give the Obama administration an opportunity to review the regulation.

By way of background, on June 6, 2008, then-President George W. Bush signed Executive Order 13,465, which instructs that "Executive departments and agencies that enter into contracts shall require, as a condition of each contract, that the contractor agree to use an electronic employment eligibility verification system designated by the Secretary of Homeland Security to verify the employment eligibility of: (i) all persons hired during the contract term by the contractor to perform employment duties within the United States; and (ii) all persons assigned by the contractor to perform work within the United States on the Federal contract." President Bush also commanded that the Federal Acquisition Regulation ("FAR"), which governs the acquisition of supplies and services by all federal agencies, be amended to incorporate the foregoing requirement. Three days later, then-Secretary of Homeland Security Michael Chertoff signed a notice designating E-Verify as the electronic employment eligibility verification system to be used by federal contractors and subcontractors.

On June 12, 2008, the agencies responsible for issuing the FAR published a proposed rule to implement Executive Order 13,465 and solicited comments on the proposed rule's text. On November 14, 2008, a final rule was published in the Federal Register with an effective date of January 15, 2009.

In addition to responding to numerous comments attacking the legality of Executive Order 13,465 and the proposed rule, the final rule explained that "[s]everal commenters suggested that E-Verify has ongoing system security problems that jeopardize the privacy

and security of individuals' personal information." The final rule also explained that "[m]any commenters stated a concern that E-Verify's inability to prevent identity theft leaves employers that use E-Verify vulnerable to sanctions." Ultimately, however, the final rule rejected these privacy-related concerns. For example, the final rule asserted that "security measures in place [to protect employees' personal information transmitted though E-Verify] include among other things both strong and limited access controls, transmission encryption, and extensive audit logging."

On December 23, 2008, the Chamber of Commerce – joined by the Associated Builders and Contractors, Inc.; the Society for Human Resource Management; the American Council on International Personnel; and the HR Policy Association – filed a Complaint for Declaratory and Injunctive Relief in the U.S. District Court for the District of Maryland. In addition to challenging the substance of the final rule, the plaintiffs contested the Executive Order, claiming it was unconstitutional and that it was an unlawful attempt to circumvent existing immigration laws. The plaintiffs also challenged the expansion of E-Verify to require the reauthorization of existing workers.

Shortly after the plaintiffs filed their complaint, the parties reached an agreement to delay implementation of the final rule until February 20, 2009, in order to allow expedited briefing on cross-motions for summary judgment. The plaintiffs' motion for summary judgment was filed on January 14, 2009, the same day that a notice appeared in the Federal Register delaying the final rule's enforcement until February 20, 2009.

On January 27, 2009 – one day before the Federal Government's deadline for responding to the plaintiffs' motion for summary judgment – the parties reached an agreement delaying the applicability date of the final rule until May 21, 2009. A notice to this effect was published in the Federal Register on January 30, 2009.[55] In addition, the Federal Government filed an emergency motion with the district court asking it to stay judicial proceedings for 90 days "in order to allow the newly-inaugurated

[55] 74 Fed. Reg. 5,621 (Jan. 30, 2009).

Administration of President Barack Obama to review the [regulations] at issue in this case." On January 28, 2009, the district court issued an order granting the Federal Government's emergency motion.

Given the significant burdens the final rule would have imposed on federal contractors and subcontractors, this most recent delay in the final rule's enforcement represents an intermediate victory for federal contractors and subcontractors throughout the United States. In addition, the Obama Administration's pledge to review the final rule may mean that privacy concerns raised by commenters will be given greater weight.

H. Prospects for Federalizing Information Security Requirements

For many of the same reasons that a federal security breach notification law is unlikely to pass during this legislative session, the prospects for federalizing information security requirements are dim. This is particularly true if legislative activity at the state level continues to target predominantly discrete and specialized aspects of information security.[56] However, increased activity at the state level with broader application, such as that which is occurring in Massachusetts, may force the hand of federal legislators. The new Massachusetts data security regulations require businesses that own, license, store or maintain personal information about Massachusetts residents to develop, implement, maintain, and monitor a comprehensive written information security program that is reasonably consistent with industry standards and that contains administrative, technical and physical safeguards to ensure the security and confidentiality of records that contain personal information. These controversial regulations are some of the first that require businesses to take specific,

[56] For example, many states have enacted laws that restrict the ways in which businesses collect, store and disclose Social Security numbers. But these laws apply specifically to Social Security numbers rather than broader categories of sensitive personal information that might also benefit from such limitations. *See, e.g.*, N.Y. GEN. BUS. LAW § 399-dd.

affirmative steps in furtherance of information security.[57] To the extent states begin adopting different requirements in this regard, businesses may push more strongly for a uniform federal solution to minimize the costs of compliance, particularly if the state requirements conflict.

News of major data security lapses, such as the recent breach at Heartland Payment Systems that potentially compromised tens of millions of credit and debit card transactions, may also provide the impetus for legislators, and the business community, to seek a federal data security solution. Such large-scale incidents underscore the importance of adequate information security mechanisms. The headlines are difficult to ignore. But if businesses fail to properly heed their warning, legislators at the federal level may seek to remedy perceived security weaknesses through legislation that, like the Massachusetts regulations, requires the regulated community to take specific, affirmative steps to protect information. Moreover, to promote greater uniformity, lawmakers may seek to replace the current sector-specific approach to data security regulation with a more comprehensive, broadly-applicable privacy and data security law, like the European Union's Data Protection Directive.[58]

---

[57] Controversy surrounding the new Massachusetts data security regulations, 201 CMR 17.00, particularly the tight compliance schedules to implement new and unprecedented information security safeguards, prompted the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") to make minor revisions to the regulations and twice delay their effective date. *See* OCABR Press Release, *New personal information security for consumers begins Jan. 1, 2010* (Feb. 12, 2009), http://www.mass.gov/. For more details on these regulations and the various compliance extensions, visit Proskauer's Privacy Law Blog at http://privacylaw.proskauer.com/.

[58] EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L 281) 31.

I. The Prospect for Increased Government Enforcement

Many believe that federal enforcement of privacy and security laws has been modest. While the FTC has brought several news-making enforcement actions, including those noted above, prosecutions in sheer number have been small. There has been little to no enforcement by other regulators, such as the Department of Health and Human Services ("HHS") Office for Civil Rights (with jurisdiction over the HIPAA Privacy Rule), and agencies other than the FTC that are responsible for Gramm-Leach-Bliley Act enforcement.

When President Obama was a candidate, he promised more vigorous enforcement with respect to privacy and data security, especially in light of the increased incidence of data security breaches and the attention being paid to identity theft. The appointment of Commissioner Leibowitz – an active privacy advocate – to chair the FTC suggests a new era of enforcement, in an environment of greater regulatory oversight in general. Moreover, despite the deferral of the effective date of the Red Flags Rules at the FTC, once they are operative, enforcement will follow. And with the passage of HITECH and its accompanying data security and breach notification obligations, enforcement by regulators at HHS is assured.