

**LABOR & EMPLOYMENT ALERT**

---

**NOT ON YOUR WATCH: RESIDENTS' PERSONAL INFORMATION PROTECTED BY MASSACHUSETTS DATA PRIVACY REGULATIONS****Implementation by March 1, 2010**

All individuals, corporations, associations, partnerships and other legal entities owning, licensing, receiving, maintaining, processing, or otherwise having access to Massachusetts residents' "Personal Information,"<sup>1</sup> irrespective of where they are located (all such individuals or entities, are "Holders" for purposes of this article), must examine the security of such Personal Information and take all necessary action to ensure compliance with the new Massachusetts regulations discussed in this article. Failure to comply may subject Holders to both public and private actions, assessments and penalties.

Although all Holders will be affected, employers and business organizations will bear the greatest burdens resulting from these new Massachusetts regulations and should take special care to ensure compliance.

**OCABR's Regulation and Its Statutory Predicates**

Massachusetts has, like most states, recently enacted data breach notice legislation requiring individuals and entities that own, license or store residents' Personal Information as computerized data to notify affected residents of unauthorized data disclosures. However, the Massachusetts statute, M.G.L. ch. 93H (the "Data Breach Law"),<sup>2</sup> goes beyond most states' legislation by directing the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") to develop minimum security requirements that all Holders must follow.<sup>3</sup>

These security requirements, set forth in regulations entitled the "Standards for the Protection of Personal Information of Residents of the Commonwealth" (201 C.M.R. 17.00 *et seq.*) (the "Standards"), require three primary safeguards for electronic and paper records containing Massachusetts residents' Personal Information:<sup>4</sup>

- (1) developing a comprehensive *written* information security program;
- (2) entering into contracts with service providers to assure *Standards* compliance; and
- (3) meeting a list of minimum security requirements for computer systems electronically storing or transmitting Personal Information.

---

<sup>1</sup> Defined below in the section entitled "Definition of Personal Information."

<sup>2</sup> The Data Breach Law provides detailed statutory requirements for responding to breaches of personal information security. Passage of M.G.L. ch. 93H was followed shortly thereafter by M.G.L. ch. 93I, the Commonwealth's law regarding the disposal of records containing Massachusetts residents' personal information. M.G.L. ch. 93I is generally intended to prevent unintended breaches of personal information security by requiring a secure disposal process. This article only addresses the *Standards*, though it highlights applicable intersection points between the *Standards* and the two statutes.

<sup>3</sup> M.G.L. ch. 93H, § 2(a).

<sup>4</sup> 201 C.M.R. 17.05.

## LABOR & EMPLOYMENT ALERT

---

### ***Standards' Purpose***

The *Standards* are designed to “safeguard” Massachusetts residents’ Personal Information. As noted by Daniel C. Crane, the former Undersecretary of OCABR, “most of the laws [and regulatory schemes of other states] only address what you can do after the horse is out of the barn.... We want to keep the horse in the barn.”<sup>5</sup> Accordingly, the Massachusetts *Standards* take a proactive approach to data security, focusing on “insider” and “outsider” threats alike.

While Massachusetts residents are the primary beneficiaries of the protections provided by the *Standards*, others also stand to benefit. Credit card companies, banks and healthcare providers – custodians of accounts containing Personal Information – support and could benefit from this sort of regulation. Why? Such custodians often, and perhaps unjustifiably, have had to pay the costs associated with frauds allowed to happen by others’ negligence; under the Data Breach Law and the new standard of care created by the *Standards*, the negligent parties will be made to pay the penalties, assessments and damages.<sup>6</sup> Simply put, the *Standards* shift data breach costs to those in control of the Personal Information.

### **Implementation Date and Selective History of Amendments**

The *Standards* will become effective on March 1, 2010. Though originally set for January 1, 2009, the *Standards’* implementation has been extended three times due, in part, to continuing stakeholder criticism, a difficult economy and internal changes at OCABR.<sup>7</sup> The most recent regulatory amendment was made in August 2009. As evidenced by a September 2009 public hearing, the latest version has been met with substantial approval by many stakeholders who previously had argued against various *Standards* concepts. OCABR clarifications and further stakeholder suggestions addressed at this public hearing suggest that further changes to the *Standards* may be in store before implementation. However, given the already numerous implementation date extensions and the tenor of current public comments, a further deadline extension is unlikely.

### **(Possible) Coming Attractions for the *Standards***

On May 12, 2009, the Massachusetts legislature held a public hearing on Massachusetts Senate Bill 173 (“**SB 173**”). SB 173 proposes changes to the Data Breach Law’s enabling language in several important respects; if passed, such changes will inevitably result in substantial modifications to OCABR’s *Standards*:

- A. OCABR’s adoption of the *Standards* would be made permissive rather than mandatory;
- B. Agencies would be added to OCABR’s purview for the *Standards’* purposes;<sup>8</sup>
- C. OCABR would be restricted from requiring any (1) “specific technology” or (2) “specific method” for protecting Personal Information;
- D. OCABR would be required, notwithstanding the *Standards’* adoption, to adopt separate regulations for “small businesses” reflecting small businesses’ “unique situation and resources;”<sup>9</sup>

---

<sup>5</sup> Kathryn Eident, *New Credit Rules Draw Criticism*, Milford Daily News, December 25, 2008, <http://www.milforddailynews.com/archive/x1142647673/New-credit-rules-draw-criticism?>

<sup>6</sup> Greg Masters, *Strictest data law in nation*, SC Magazine US, January 1, 2009, <http://www.scmagazineus.com/Strictest-data-law-in-nation/article/123432/> (quoting Avivah Litan).

<sup>7</sup> OCABR has restated its *Standards*, and extended the compliance timeline, on November 14, 2008, February 12, 2009, and August 17, 2009.

<sup>8</sup> M.G.L. ch. 93H, § 1(a) defines “Agency” as “any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision hereof.”

<sup>9</sup> The term “small business” is not defined in SB 173.

## LABOR & EMPLOYMENT ALERT

---

- E. Holders “required to comply” with federal “laws, rules, regulations, guidance, or guidelines” for protecting Personal Information would be given safe harbor treatment through presumptive compliance; and
- F. Employees who willfully violate the *Standards*, the Data Breach Law or any written information security program issued by a “person covered by state or federal privacy laws” could be terminated from employment for this “just cause.”

Taking office only days before SB 173’s public hearing (and months before issuing the August 2009 *Standards* amendment), new OCABR undersecretary Barbara Anthony commented that “[the proposed amendment to the Data Breach Law] does not contain the same scope of consumer protections that our enabling legislation does.”<sup>10</sup> Indeed, the revisions proposed by SB 173 undercut some of the more ambitious goals of earlier versions of the *Standards*. However, since OCABR’s August 2009 amendments already address (albeit in different ways) many of the provisions targeted by SB 173, it is unclear whether action regarding SB 173 will be a legislative priority. Popular support regarding the SB 173 issues that remain outstanding, notably (B) and (F), above, may help to keep some momentum alive. Unquestionably, however, the urgency associated with such changes has diminished.

### **National Impact of the *Standards***

The *Standards* represent one of the most forceful lawmaking attempts to date to promote information privacy and data security. Collected by myriad businesses nationwide, Massachusetts residents’ Personal Information is a fairly common data element. Due to (i) OCABR’s aggressive, prevention-focused approach and (ii) the prevalence and pervasiveness of Massachusetts residents’ Personal Information all over the country, the Commonwealth’s *Standards* could become a national data security blueprint. Indeed, given the Obama administration’s campaign commitment to privacy issues, Massachusetts’ *Standards* may be watched and/or copied closely as a model for national legislation along similar lines.

### **Broad Reach of the *Standards***

All Holders owning, licensing, receiving, maintaining, processing, or otherwise having access to Personal Information “in connection with the provision of goods or services or in connection with employment” of even a single Massachusetts resident are subject to the *Standards*.<sup>11</sup> OCABR’s *Standards* do not end at the Massachusetts state line; they reach across state boundaries to cover out-of-state Holders. OCABR also has not shied away from imposing the *Standards* on industries already regulated by the federal

---

<sup>10</sup> Alexander B. Howard, *Mass. Senate seeks to amend, weaken data breach notification law*, SearchCompliance.com, May 14, 2009,

[http://searchcompliance.techtarget.com/news/article/0,289142,sid195\\_gci1356356,00.html](http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1356356,00.html) (quoting Barbara Anthony).

<sup>11</sup> 201 C.M.R. 17.02, 17.03(1). As noted in OCABR’s FAQ, the *Standards* apply “to those engaged in commerce.” See Frequently Asked Questions Regarding 201 C.M.R. 17.00,

<http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf> (the “FAQ”). Also, Massachusetts state government agencies, executive offices, departments, boards, commissions, bureaus, divisions and authorities, all excluded from the definition of “person,” are covered by the Massachusetts governor’s Executive Order No. 504: “all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus and offices, now existing and hereafter established.” Exec. Order No. 504, (Mass. Sept. 19, 2008), <http://www.mass.gov/Eoca/docs/idtheft/eo504.pdf>; see also M.G.L. ch. 93H, §§ 2(b) and (c). The FAQ specifically notes that municipalities are excluded from the definition of “person.”

## LABOR & EMPLOYMENT ALERT

---

government, other state governments or foreign governments.<sup>12</sup> Compliance with existing regulatory requirements for protecting records containing Personal Information does not obviate the need to comply with Massachusetts' *Standards* – and, *vice versa* – mere compliance with the Massachusetts *Standards* may be insufficient if another, more protective, framework also applies. As discussed later in this article, the validity of this wide reach may be questioned. At least for now, however, full compliance with applicable requirements demands that all Holders identify and adopt the strictest and/or most protective requirements.<sup>13</sup> Holders currently compliant with data security standards either developed within the private sector by industry groups (such as the Payment Card Industry Security Standards Council)<sup>14</sup> or mandated by federal laws and regulations<sup>15</sup> will have a head start on compliance with the Massachusetts' *Standards*. However, even these Holders will have work to do to ensure *Standards* compliance.<sup>16</sup>

It is important to remember that full compliance with the letter and spirit of the *Standards* is required but does not provide any “safe harbor” treatment in the event of a data breach.<sup>17</sup> Nevertheless, compliance is a key risk-reduction tool. A fully compliant Holder will not only be better protected against, and more prepared to respond to, a data breach, but it will also be more likely to withstand claims of negligence by affected individuals and finger-pointing deep-pockets, such as credit card companies, banks and healthcare providers.

---

<sup>12</sup> Exceptions contained in the “personal information” definition may provide some limited leeway such as for publicly available records. 201 C.M.R. 17.02.

<sup>13</sup> M.G.L. ch. 93H, § 5; 201 C.M.R. 17.03(1).

<sup>14</sup> The Payment Card Industry Security Standards Council (PCI) developed PCI DSS, the Payment Card Industry Data Security Standard, in 2006 and has updated it since then. PCI is the union of various cardholder security initiatives from several major credit card companies; its mission is heightening cardholder security by mandating minimum merchant standards for protecting cardholder data. A detailed examination of industry standards in connection with the *Standards* is beyond this article's scope.

<sup>15</sup> Such regulations include, without limitation, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Financial Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act or GLBA), the Sarbanes-Oxley Act of 2002 (SOX), and the Fair and Accurate Credit Transactions Act of 2003 (FACTA) (and its associated “Red Flag Rules” as published by the Federal Trade Commission). A discussion of these laws and regulations and their bearing upon the *Standards* is beyond the scope of this article. OCABR has expressly noted that compliance with HIPAA does not exempt a Holder from compliance with the *Standards*. See the FAQ.

<sup>16</sup> Users of swipe technology only – without retaining or storing any Personal Information – would not own or license Personal Information for the *Standards*' purposes if the swiped data is batched out in accordance with PCI DSS. See the FAQ.

<sup>17</sup> The safe harbor actually provided in Section 5 of the Data Breach Law is quite narrow and does not impact a Holder's compliance efforts for purposes of the *Standards*. In the event of an actual breach of security, a Holder will be presumed compliant with the Data Breach Law if it: (1) “maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines;” (2) notifies affected Massachusetts residents pursuant to such procedures when a breach occurs; and (3) notifies Massachusetts' attorney general and OCABR's undersecretary as soon as practicable and without unreasonable delay following the breach. M.G.L. ch. 93H, § 5.

## LABOR & EMPLOYMENT ALERT

---

### Definition of Personal Information

As set forth in both the Data Breach Law and the *Standards*, “Personal Information” means:

a Massachusetts resident’s  
first name (or first initial) and last name

used *in combination with*  
such resident’s

Social Security number,  
driver’s license number, or  
any financial account number,  
debit account number, or  
credit card number.<sup>18</sup>

If such information is lawfully obtained from (i) publicly available information or (ii) federal, state or local government records, it is excluded from the definition of “Personal Information” for both the Data Breach Law and the *Standards*.<sup>19</sup>

### Comprehensive Written Information Security Program

Every Holder must develop, implement and maintain a comprehensive written information security program (“WISP”) to protect Personal Information.<sup>20</sup> WISPs must be consistent with the various state and federal regulations by which such Holders may be regulated.<sup>21</sup> Further, WISPs must safeguard the security and confidentiality of Personal Information – administratively, technically and physically.<sup>22</sup>

Pursuant to the latest iteration of the *Standards*, Holders drafting a WISP are permitted some discretion to develop safeguards that are appropriate in light of relevant surrounding circumstances. Specifically, a

---

<sup>18</sup> M.G.L. ch. 93H, § 1; 201 C.M.R. 17.02. This information need not be accompanied by the resident’s security/access code, personal identification number or password for inclusion as “personal information.” 201 C.M.R. 17.02. Regarding “financial accounts,” the definition set forth in the FAQ is broad: “an account that if access is gained by an unauthorized person to such account, an increase of financial burden, or a misappropriation of monies, credit or other assets could result.” Examples provided by the FAQ are narrower: a “checking account, savings account, mutual fund account, annuity account, any kind of investment account, credit account or debit account.” An account number like an insurance policy number is a judgment call; whether or not it is a “financial account” for purposes of the *Standards* requires an analysis based on the definition, above. See the FAQ.

<sup>19</sup> The M.G.L. ch. 93I (disposition of records) definition of “personal information” includes biometric indicators (such as fingerprints and retinal scans). Therefore, extra caution should be exerted when disposing of biometric indicators. In addition, there is no exclusion for publicly available information and records as there is in the Data Breach Law and the *Standards*. See generally, M.G.L. ch. 93I, § 1.

<sup>20</sup> 201 C.M.R. 17.03(1). See 201 C.M.R. 17.03(2)(a)-(j) and 17.04. In addition, Section 17.03(1) now provides that the WISP may be “written in one or more readily accessible parts.”

<sup>21</sup> 201 C.M.R. 17.03(1). The *Standards* impose an ongoing obligation to adhere to their “best practices” intent. The August 2009 amendments omitted a requirement that “industry standards” be met in addition to state and federal regulations. Although incorporating extrinsic regulatory requirements in this manner could complicate administration and enforcement, omission of “industry standards” makes this requirement more palatable.

<sup>22</sup> 201 C.M.R. 17.03(1).

## LABOR & EMPLOYMENT ALERT

---

WISP drafter (as well as the OCABR and the Massachusetts Attorney General's office) must take into account the following "risk-based" factors:<sup>23</sup>

- (a) the size, scope and type of business of the person obligated to safeguard the personal information under a WISP;
- (b) the amount of resources available to such person;
- (c) the amount of stored data; and
- (d) the need for security and confidentiality of both consumer and employee information.

As stated by OCABR Undersecretary Barbara Anthony:

"Whether it's a small amount of employee paperwork, or a large amount of consumer information kept on an electronic database, each requires its own appropriate level of security and protection...."<sup>24</sup>

Discussing what compliance means for a pizza parlor, former Undersecretary Daniel C. Crane stated: "People need to sit down and spend fifteen, twenty minutes looking at where that info is and what is needed to protect it.... That type of small business has a series of very simple, low-tech solutions to meet the regulations."<sup>25</sup> If this business had employee information only – and its few employees accepted cash exclusively – a WISP and a locked storage cabinet within a locked back office are likely appropriate.<sup>26</sup> While 15-20 minutes may be sufficient to formulate the bare outline of a pizzeria's compliance plan, most Holders will likely need to spend far more time to assess and address their security compliance.<sup>27</sup>

### Minimum WISP Requirements

At a minimum, all of the actions identified below in A, B, and C are required WISP elements:<sup>28</sup>

---

<sup>23</sup> See also M.G.L. ch. 93H, § 2(a). As stated in the Press Release, such changes "make clear the regulations are risk-based in implementation, not just in enforcement as had been the case in earlier versions of the regulations."

<sup>24</sup> See the Press Release, quoting OCABR Undersecretary Barbara Anthony.

<sup>25</sup> Jackie Noblett, *Critics: Data law tying up businesses*, Boston Business Journal, December 5, 2008, <http://boston.bizjournals.com/boston/stories/2008/12/08/story1.html> (quoting OCABR Undersecretary Daniel C. Crane).

<sup>26</sup> See the FAQ.

<sup>27</sup> For instance, approaches for a business with more than a few employees and, perhaps, some customer information would be more stringent and *even more stringent* with *more personal information* in play. There should be a correlation between the (1) protection efforts undertaken and (2) the relevant Section 17.03(1) factors associated with the Personal Information protected.

<sup>28</sup> Three important minimum WISP requirements were entirely omitted by the August 2009 amendment to the *Standards*:

1. Limit the amount of Personal Information collected, and the retention period for such information, to a level "reasonably necessary to accomplish the legitimate purpose for which it is collected;" and
2. Identify: (i) paper, electronic and other records containing Personal Information and (ii) computer systems, laptops, portable devices and other media used to store Personal Information.
3. Restrict access to Personal Information to personnel "reasonably required to know" such information in order to (i) achieve the "legitimate purpose for which it is collected" or (ii) comply with state or federal record retention requirements;

## LABOR & EMPLOYMENT ALERT

---

### A. *Implementing, Monitoring and Evaluating a WISP*

1. Designate one or more employees with responsibility for WISP maintenance and oversight;<sup>29</sup>
2. Identify and assess reasonably foreseeable security risks (both internal and external) to electronic, paper and other records containing Personal Information;<sup>30</sup>
3. Establish and maintain a computer security system as further described in the section entitled “Computer Security System Requirements,” below;<sup>31</sup>
4. Monitor the WISP regularly to ensure operation “reasonably calculated to prevent unauthorized access to or use of” Personal Information and periodically upgrade security measures as necessary;<sup>32</sup>
5. Review security measures not less than annually – or more frequently if there are material changes in business practices that impact Personal Information security or record integrity;<sup>33</sup>
6. Evaluate and undertake necessary improvements to increase the WISP’s effectiveness by: (i) implementing employee training programs; (ii) monitoring employee compliance with WISP rules; and (iii) improving detection and prevention of security system failures;<sup>34</sup> and
7. Review and enhance business practices and the WISP by documenting security breaches, including conducting post-incident reviews of events and actions taken.<sup>35</sup>

### B. *Personnel Accessing Personal Information*

1. Restrict physical access to records containing Personal Information and storing such records and data in locked facilities, storage areas or containers;<sup>36</sup>
2. Develop employee security policies relating to storage, access and transport of records containing Personal Information off business premises;<sup>37</sup>
3. Impose disciplinary measures for WISP rule violations;<sup>38</sup> and

---

As OCABR points out in its August 2009 FAQ, these “good business practice” requirements have been omitted as they are obvious compliance steps and, therefore, unnecessary to mandate. They “will be used as a form of guidance only.”

<sup>29</sup> 201 C.M.R. 17.03(2)(a).

<sup>30</sup> 201 C.M.R. 17.03(2)(b).

<sup>31</sup> 201 C.M.R. 17.04 and, to a lesser extent, 17.03(2)(b)(3) with respect to detecting and preventing security system failures.

<sup>32</sup> 201 C.M.R. 17.03(2)(h). Parties commenting on the *Standards* noted that access monitoring, though a laudable goal, is a hugely expensive undertaking, especially because of its redundancy with properly administered authorizations and access controls. *See also* 201 C.M.R. 17.04(4).

<sup>33</sup> 201 C.M.R. 17.03(2)(i).

<sup>34</sup> 201 C.M.R. 17.03(2)(b)(1-3). Regarding employee training, per the FAQ, there is no “basic standard.” Holders must do enough to ensure that employees with Personal Information access know their obligations to protect such Personal Information.

<sup>35</sup> 201 C.M.R. 17.03(2)(j). The term “breach of security” is defined in both the Data Breach Law and the *Standards* as “the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.” M.G.L. ch. 93H, § 1; 201 C.M.R. 17.02.

<sup>36</sup> 201 C.M.R. 17.03(2)(g). Holders must develop reasonable WISP exceptions to accommodate use of Personal Information records in connection with laptops and “other portable devices” that are otherwise used in a manner compliant with the *Standards*.

<sup>37</sup> 201 C.M.R. 17.03(2)(c). *See also* Subsection A, Number 3 of this Section. This section clearly implicates employees working from home or otherwise working remotely.

## LABOR & EMPLOYMENT ALERT

---

4. Restrict terminated personnel from access to physical and electronic records.<sup>39</sup>
- C. Third Party Service Providers Accessing Personal Information

The *Standards* require that Holders oversee service providers with Personal Information access by:

1. selecting and retaining only those service providers that are capable of maintaining appropriate security measures to protect Personal Information consistent with the *Standards* and any applicable federal regulations;<sup>40</sup> and
2. requiring, by contract, that such service providers implement and maintain appropriate security measures to protect Personal Information consistent with the *Standards* and any applicable federal regulations.<sup>41</sup>

OCABR's requirement that Holders obtain contracts regarding compliance from service providers recently reappeared after a seven-month absence from the *Standards*.<sup>42</sup> The current version, reincorporated by the August 2009 amendments, is modeled on the Federal Trade Commission's well-received Safeguards Rule.<sup>43</sup> Holders should take note that a two-year grace period makes this requirement generally (but not entirely) prospective. The current forward-looking plan is a great improvement over prior requirements requiring compliance on "day one."<sup>44</sup> Until March 1, 2010, service provider contracts need not contain provisions promising *Standards* compliance; however, compliance provisions must be on everyone's contract checklists by the *Standards*' effective date. The grace period has obviated the eleventh hour act of revisiting and reworking established contractual arrangements that otherwise would have been necessary for timely compliance.

### Computer Security System Requirements

Section 17.04 of the *Standards* enumerates minimum requirements for computer systems that electronically store or transmit Personal Information. All computers, laptops and other electronic devices storing or transmitting Personal Information, including transmissions via wireless systems, are addressed.

---

<sup>38</sup> 201 C.M.R. 17.03(2)(d).

<sup>39</sup> 201 C.M.R. 17.03(2)(e). Note that password and user name deactivation is no longer mandated by the *Standards* (but remains good business practice).

<sup>40</sup> 201 C.M.R. 17.03(2)(f)(1).

<sup>41</sup> 201 C.M.R. 17.03(2)(f)(2). In Section 9 of Executive Order No. 504, there is an analogous provision for contracts entered into by Massachusetts state agencies. Exec. Order No. 504, (Mass. Sept. 19, 2008), <http://www.mass.gov/Eoca/docs/idtheft/eo504.pdf>. It is unclear whether this provision will be modified consistent with OCABR's most recent amendments to the *Standards*.

<sup>42</sup> The August 2009 *Standards* amendment defined "service provider" as "any person that receives, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation." OCABR's definition also provides that "'service provider' shall not include the U.S. Postal Service." Importantly, the definition provides two limits on potential classification as a "service provider;" specifically, a potential "service provider" must: (i) have some access to Personal Information; and (ii) directly provide services to a Holder.

<sup>43</sup> 16 CFR Part 314.

<sup>44</sup> For longer-term contracts (including those already executed), contracts must be amended to comply with the *Standards* by March 1, 2012, when the beneficial effects of the grace period sunset.

## LABOR & EMPLOYMENT ALERT

---

Such devices and systems must be protected by a security system incorporating – “to the extent technically feasible” – all of the following base elements:<sup>45</sup>

1. Authentication. Secure user authentication protocols, including: (i) control over user IDs and other identifiers; (ii) reasonably secure password assignment and selection methodology;<sup>46</sup> (iii) control over, and secured storage and/or formatting of, all data security passwords; (iv) restrictions on access to active users and active user accounts; and (v) denial of login access after multiple failed attempts.<sup>47</sup>
2. Access Control. Secure access control measures that: (i) restrict access to Personal Information to personnel who require such information to perform job duties;<sup>48</sup> (ii) “reasonably design” institutional IDs and passwords in a manner that is calculated to maintain the integrity of access control security;<sup>49</sup> and (iii) assign a unique ID and password (not vendor-supplied default passwords) to each person with computer access.<sup>50</sup>
3. Monitoring. Reasonable system monitoring for unauthorized use of, or unauthorized access to, Personal Information.<sup>51</sup>
4. Firewall. For records containing Personal Information on an Internet-linked system (physically or wirelessly), reasonably up-to-date firewall protection and operating system security patches reasonably designed to maintain Personal Information integrity.<sup>52</sup>
5. System Security. Reasonably up-to-date versions of system security agent software, with malware and virus protection, which are diligently maintained and upgraded.<sup>53</sup>
6. Device Encryption. Encryption of all Personal Information that is stored on laptops or other portable devices.<sup>54</sup>
7. Transmittal Encryption. Encryption of all data containing Personal Information that will be transmitted across public networks or transmitted wirelessly.<sup>55</sup>
8. Education & Training. Employee education and training on (i) proper use of computer security system and (ii) importance of Personal Information security.<sup>56</sup>

---

<sup>45</sup> OCABR’s August 2009 amendments left the *Standards’* Section 17.04 computer system security requirements generally untouched – adopting only an overarching “to the extent technically feasible” limitation for computer system security. The August 17, 2009 FAQ defines this feasibility concept: “Technically feasible” means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.” See the FAQ. In other words, if it must be done and the technology reasonably exists to do it, then that technology must be used. However, the FAQ points out that other, perhaps less technical, methods may be employed in order to ensure Personal Information security.

<sup>46</sup> The *Standards* permit use of unique identifier technologies, such as biometrics or token devices, as an alternative to familiar requirements pertaining to password “strength” such as length, avoidance of common words or numbers, and case and character differentiation.

<sup>47</sup> 201 C.M.R. 17.04(1)(a)-(e).

<sup>48</sup> 201 C.M.R. 17.04(2)(a).

<sup>49</sup> 201 C.M.R. 17.04(2)(b).

<sup>50</sup> 201 C.M.R. 17.04(2)(b).

<sup>51</sup> 201 C.M.R. 17.04(4). See also C.M.R. 17.03(2)(h).

<sup>52</sup> 201 C.M.R. 17.04(6).

<sup>53</sup> 201 C.M.R. 17.04(7).

<sup>54</sup> 201 C.M.R. 17.04(5).

<sup>55</sup> 201 C.M.R. 17.04(3). The caveat “to the extent such encryption is technologically feasible” was originally set forth in the *Standards’* 201 C.M.R. 17.04(3) regarding transmittal encryption only; no similar caveat was provided with respect to device encryption in 201 C.M.R. 17.04(5). Because universal adoption of both device and transmittal encryption were deemed to be hindered by technological obstacles, all of Section 17.04 was conditioned by the technical feasibility proviso discussed later in this article.

## LABOR & EMPLOYMENT ALERT

---

### “Encryption” Redefined by August 2009 Amendments

August 2009 changes to the definition of “encrypted” will permit Holders to use a wider array of defensive technologies than previously contemplated. While prior iterations of the *Standards* had required the use of an algorithmic encryption process, the latest requirement is limited to altering data to a state “in which meaning cannot be assigned without the use of a confidential process or key.”<sup>57</sup> Although a confidential process or key is still required, the *Standards* no longer mandate an algorithmic lock. By broadening this encryption standard, OCABR has significantly eased its prior encryption requirements, making them, (per the FAQ):

“technology neutral so that as encryption technology evolves and new standards are developed, this regulation will not impede the adoption of new technologies.”

Despite the seemingly broad language of the change, however, Holders should not equate “encrypted” with “password-protected.” To the contrary, password protection does not alter the underlying data but only restricts access to it; therefore, passwords do not provide acceptable protection even under the less-stringent requirement.

### Failure to Comply

In addition to general OCABR oversight, the Massachusetts Attorney General has multiple enforcement options available for use against non-compliant Holders. For example, enforcement could include action under the Commonwealth’s consumer protection statute (M.G.L. ch. 93A) seeking: (i) injunctive relief regarding continuing noncompliance; (ii) restitution for ascertainable loss of money and property; and/or (iii) assessment of fines for each method, act or practice violating the Data Breach Law and/or the *Standards* (up to a \$5,000 fine for each violation an offender “knew or should have known” to be in violation, plus attorneys’ fees and the reasonable costs of investigation and litigation).<sup>58</sup> It remains to be seen whether penalties will be assessed on a per-Holder, per-resident or per-data item basis. In addition, for willful violations, amounts imposed for restitution may be multiplied by a factor between two and three.<sup>59</sup>

It remains unclear whether, in the absence of a data breach, the Attorney General will target out-of-state companies holding Massachusetts residents’ Personal Information for enforcement of technical requirements. Such broad policing of compliance would require an enormous amount of resources that may be unavailable in an economy that is struggling through a long recovery period. Presumably, a breach of security with respect to Personal Information will spark the Attorney General’s interest irrespective of geographic origin; time will show whether the difficulties of long-arm enforcement will dampen such interest.<sup>60</sup>

---

<sup>56</sup> 201 C.M.R. 17.04(8).

<sup>57</sup> 201 C.M.R. 17.02.

<sup>58</sup> M.G.L. ch. 93H, §6; M.G.L. ch. 93A, § 4.

<sup>59</sup> M.G.L. ch. 93A, § 4.

<sup>60</sup> M.G.L. ch. 93H, § 5. The term “breach of security” is defined in M.G.L. ch. 93H, §1. The safe harbor from Section 5 of the Data Breach Law is discussed at Note 17. Failure to comply fully with the Data Breach Law and *Standards* dispels any protection provided by the safe harbor. M.G.L. ch. 93H, § 5.

## LABOR & EMPLOYMENT ALERT

---

In addition to triggering state action, non-compliance with OCABR's *Standards* may also result in private actions and unanticipated costs.<sup>61</sup> Non-compliance with the high standard of care established by the *Standards* may be used as evidence of negligence in a civil action brought by an affected plaintiff – to “persuade judges and juries that organizations that lost data are negligent.”<sup>62</sup> Affected plaintiffs may also demand that Holders compensate them for costs and damages associated with fraud stemming from a data breach. Further, violating this regulatory framework (where no framework previously existed) may render breaches of security and associated defense costs uninsurable under standard commercial general liability policies – or even many cyber risk policies – without special endorsements.<sup>63</sup>

### Open Issues to Consider

Realizing the main goals of the Data Breach Law and the *Standards* – identity theft prevention and safeguarding Personal Information – is in the best interest of all stakeholders.<sup>64</sup> Identity theft victims are subjected to significant inconvenience and financial harm; criminal elements worldwide may gain surreptitious access to Personal Information; Holders' goodwill with customers, stockholders and industry partners is perhaps unredeemably undermined; and all citizens' confidence in “the system” – government, business and consumer-inclusive – is shaken when a data breach is detected.

Holders must recognize that they hold Personal Information in a fiduciary capacity and could be held accountable for negligent data security practices. Properly addressing the concerns and interests of all stakeholders requires a reasonable balance to guide data security policy decisions. The expense of protecting Personal Information should not take precedence over individual privacy rights. Nor should custodians of financial accounts be required to act as insurers of businesses' data privacy practices.

As yet, neither the Data Breach Law nor the *Standards* have been interpreted by any court of law. Both have, however, been closely examined by many members of the business community – as demonstrated during the notice and comment periods for multiple iterations of the *Standards*. Although OCABR took community feedback into account in its February and August 2009 amendments by making significant changes, remaining open issues must be considered and addressed – if not by OCABR, then by Holders responsible for regulatory compliance. Some of those significant issues are discussed below.

---

<sup>61</sup> With respect to private actions, the Data Breach Law specifies in Section 6 that “the *attorney general* may bring an action” [*emphasis added*] pursuant to M.G.L. ch. 93A, § 4 to “remedy violations of this chapter and for other relief that may be appropriate.” While there is no express authorization for consumer recourse to private M.G.L. ch. 93A remedies under Sections 9 and 11, general civil litigation may spring from OCABR's *Standards*. See also Testimony of Bill Vernon, State Director, National Federation of Independent Business (NFIB), before The Office of Consumer Affairs and Business Regulation (January 16, 2009), [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) (the “NFIB Testimony”) (failure to bar M.G.L. ch. 93A private actions could engender litigation).

<sup>62</sup> Greg Masters, *Strictest data law in nation*, SC Magazine US, January 1, 2009 <http://www.scmagazineus.com/Strictest-data-law-in-nation/article/123432/> (quoting Phil Neray).

<sup>63</sup> Note that there is a burgeoning market for insurance covering a variety of cyber risks, most of which will require an initial security assessment. Companies considering insuring some of their risks in this area must review policy language carefully as coverages vary widely. Given the many uncertainties associated with the statute, parties should be skeptical of assurances of “coverage” under given policy language. Mark Silvestri, *Dealing with cyber risk: Closing the gaps in protection*, 28 J. Healthcare Risk Mgmt. 23, 25-26 (2009).

<sup>64</sup> Testimony of Christopher R. Anderson, President, Massachusetts High Technology Council, Inc. (MHTICI), before The Office of Consumer Affairs and Business Regulation (January 16, 2009), 2, [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) (the “MHTICI Testimony”).

## LABOR & EMPLOYMENT ALERT

---

### 1. *Timeline for Compliance.*

Compliance timeline issues previously brought to OCABR's attention have been alleviated somewhat by several deadline extensions spanning fourteen months. In addition, OCABR's August amendments' most recent extension of time permits Holders to balance the costs of compliance over multiple fiscal years. Similarly, a grace period permits Holders additional time for compliance with the new service provider contract requirement.<sup>65</sup> Nevertheless, deployment of fully-compliant security systems will be neither quick nor easy for any Holder – as anyone who has ever experienced a corporate rollout of new technology can attest. Further complicating the compliance timeline will be the inevitable flood of Holders taking action during the weeks approaching March 1, 2010. Holders are well-advised to reach compliance before this eleventh-hour rush.

### 2. *Consistency with Other Laws and Regulations.*

With their ambitious WISP requirement and associated technical and security requirements, the *Standards* appear to eclipse current legal requirements in the United States and, as a result, are poised to create multi-jurisdictional compliance challenges.<sup>66</sup> Holders that operate nationally and globally must adhere to various local, state, federal and international legal authorities – soon to include the *Standards*. Where the *Standards* conflict with other legal authorities, Holders may face duplication of efforts, wasted resources, confusion and undue complexity.

Many commentators have agreed that setting such a high bar, particularly relating to federal regulations, does not appear to have been the Massachusetts legislature's original intent.<sup>67</sup> To the contrary, the Data Breach Law mandated that regulations should be "consistent with the safeguards for protection of personal information set forth in the federal regulations" applicable to the Holder.<sup>68</sup> Instead of

---

<sup>65</sup> 201 C.M.R. 17.03(2)(f)(2).

<sup>66</sup> The Massachusetts legislature addressed the need for consistency with other states' laws and regulations in the context of SB 173.

<sup>67</sup> See Statement of Daniel J. Foley, Jr., Vice President of Government Affairs and General Counsel, Massachusetts Association of Insurance Agents (MAIA), before The Office of Consumer Affairs and Business Regulation (January 16, 2009), 4, [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) (the "MAIA Statement"); Statement of David E. Floren, Senior Vice President, Massachusetts Bankers Association (MBA), before The Office of Consumer Affairs and Business Regulation (January 16, 2009), 2, [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) (the "MBA Statement"); Letter of Marylou Buise, M.D., President, Massachusetts Association of Health Plans (MAHP), to Daniel C. Crane, Undersecretary, Office of Consumer Affairs and Business Regulation (January 16, 2009), 1, [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) (the "MAHP Letter"); Letter of Andrew J. Calamare, President and Chief Executive Officer, Life Insurance Association of Massachusetts (LIAM), to Daniel C. Crane, Director, Office of Consumer Affairs and Business Regulation (January 16, 2009), 1-2, [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) (the "LIAM Letter"); Statement of Francis C. O'Brien, Vice President, Regional Manager and Counsel, Property Casualty Insurance Association of America (PCIAA), before The Office of Consumer Affairs and Business Regulation (January 16, 2009), 1, [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) (the "PCIAA Statement"); and Statement of John P. Murphy, American Insurance Association (AIA), before The Office of Consumer Affairs and Business Regulation (January 16, 2009), 6, [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) (the "AIA Statement")

<sup>68</sup> M.G.L. ch. 93H, § 2(a).

## LABOR & EMPLOYMENT ALERT

---

implementing regulations that were consistent with federal standards, however, OCABR has burdened Holders with ensuring that their WISPs comply with both the *Standards* and any applicable state or federal regulations.

Though the overarching concern regarding regulatory consistency remains, the flexibility added by OCABR's most recent amendment has to some extent lessened its urgency. By hard-wiring Holder-specific factors into Section 17.03(1)'s WISP requirement, permitting WISPs of "one or more readily accessible parts"<sup>69</sup> and omitting "good business practice"<sup>70</sup> elements from the *Standards*, OCABR permits Holders greater leeway in tailoring WISPs to regulations that currently apply to them (which regulations may already have their own particular WISP requirements). If enforcement is approached based on OCABR's most recent *Standards*, gone is the prescriptive, one-size-fits-all approach to WISPs.

### 3. Issues Associated with Encryption.

The August 2009 amendments ably resolved several of the significant practical problems created by OCABR's original encryption requirement.<sup>71</sup> By expanding the "technical feasibility" concept to cover all computer system security requirements, Holders need only upgrade where technically feasible to do so. By modifying the definition of "encryption," OCABR has cleared the way for new technologies. That said, at least one important issue remains.

Once in place, use of encryption technologies in accordance with the *Standards* – total encryption across public networks and wirelessly – may disrupt Holders' common business practices where Personal Information is concerned.<sup>72</sup> Encrypting e-mails transmitted over a public network will render them unreadable by recipients who (i) do not have a key to access such encrypted communications and/or (ii) do not share the Holders' applicable encryption software.<sup>73</sup> Many Holders communicate with customers by e-mail and, given the nature of consumer relationships in the age of e-commerce, many of those communications will contain Personal Information.<sup>74</sup> Holders must find alternative means of transmitting such Personal Information if no available technology can secure e-mail transmissions, such as developing a secure website for client access.<sup>75</sup>

### 4. Inventorizing, Collection and Retention of Personal Information.

---

<sup>69</sup> 201 C.M.R. 17.03(1).

<sup>70</sup> See the FAQ.

<sup>71</sup> Such problems included, without limitation, system interoperability, undue taxation of Holder resources, and a requirement that Holders use algorithmic encryption technology.

<sup>72</sup> Note that although not specifically addressed, the *Standards* appear to implicate telephone communications as well, including with respect to wirelessly transmitted data containing Personal Information. 201 C.M.R. 17.01. Given the point-to-point nature of some telephone communications across telephone lines, risk is limited but worthy of consideration; wireless telephone communications issues should be considered as well.

<sup>73</sup> Letter from Steven Michalove, CISM, CISSP, Microsoft Corporation, to Daniel Crane, Undersecretary of OCABR (January 15, 2009), [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf).

<sup>74</sup> Testimony of Jon B. Hurst, President, Retailers Association of Massachusetts (RAM), before The Office of Consumer Affairs and Business Regulation (January 16, 2009), [http://www.mass.gov/Eoca/docs/idtheft/phtranscript\\_20090116.pdf](http://www.mass.gov/Eoca/docs/idtheft/phtranscript_20090116.pdf) ("RAM Testimony"); *AIA Statement*, at 4.

<sup>75</sup> See the FAQ.

## LABOR & EMPLOYMENT ALERT

---

The business community flagged numerous issues with OCABR's inventory requirement as set forth in previous iterations of the *Standards*. Seemingly putting the issue to rest, OCABR deleted these requirements in its August 2009 amendments – noting that they remained “good business practice.”<sup>76</sup> These issues warrant mention because, notwithstanding their omission, they remain an intermediate step on the path to *Standards* compliance; although OCABR may not fault the inventory process used, it may yet fault the flawed end result.

Holders inventorying records containing Personal Information for the first time face a prodigious – and ongoing – task requiring significant time and organizational resources.<sup>77</sup> By omitting the inventory mandate from the most recent *Standards*, OCABR permits Holders to create their own compliance approach and refrains from dictating the unworkable standard of an exhaustive Personal Information inventory. Similarly, by omitting a requirement that Personal Information collection be limited, OCABR has permitted Holders to take a common sense, risk-reward approach to collecting and retaining Personal Information.

While OCABR has incorporated additional flexibility into its regulation, adherence to good business practices is the *sine qua non* of *Standards* compliance. Risk-conscious Holders must be cognizant of Personal Information to which they have access and must sensibly limit its intake and retention irrespective of a lawful mandate.

### 5. Service Provider Contract Requirements.

The August 2009 amendments generally sought to align the *Standards* with the Data Breach Law's goals – in most cases retreating from earlier, more prescriptive positions. The resurgent service provider contract requirement is one of few exceptions and will undoubtedly impose new transactional costs upon both Holders and service providers. It is an absolute requirement seemingly at odds with new WISP requirements tailoring other compliance requirements to Holder-specific factors.<sup>78</sup> OCABR points out in its FAQ that this contracts provision has been adapted from the FTC's Safeguards Rule; notably, however, the Safeguards Rule applies to “financial institutions” – a class of business entity much more sophisticated (and financially positioned for compliance) than most Holders. Indeed, typical Holders will encounter numerous obstacles including the initial difficulty of introducing the new requirement into boilerplate documents for out-of-state and international service providers. In light of these considerations, perhaps OCABR may read additional flexibility into this requirement.<sup>79</sup>

OCABR's latest contract requirement is more Holder-friendly than its antecedents; (1) it permits a two-year grace period for compliance; and (2) by specifying that “provision of services directly [to a Holder]” is a prerequisite for classification as a “service provider,” OCABR has laid to rest any question of a

---

<sup>76</sup> See the FAQ.

<sup>77</sup> *AIA Statement*, at 5 and 9.

<sup>78</sup> The contract provision requires that service providers use “appropriate security measures,” so the 201 C.M.R. 17.03(1) risk-based factors would be used in that context; however, more fact-specific language permitting Holder flexibility for the overall requirement is absent from this part of the *Standards*.

<sup>79</sup> As Tami Salmon of the Investment Company Institute (ICI) pointed out in the September 2009 public hearing before OCABR, the breadth of the new definition of “owns or licenses,” discussed in further detail below, may obviate the contract requirement altogether because such service providers, having access to Personal Information, would have already been pulled into the orbit created by the *Standards*' broad language.

## LABOR & EMPLOYMENT ALERT

---

Holder's responsibility to ensure compliance down the line of service providers – only the direct relationships count. Nevertheless, the contract requirement imposes difficult new hurdles.

### 6. *OCABR's Data Breach Law Mandate Exceeded.*

Comparing the Data Breach Law and the *Standards* side-by-side has left reviewers with unanswered questions about whether the *Standards* exceed their statutory mandate. The August 2009 amendment addressed some of the inconsistencies and bound the *Standards* more closely to the Massachusetts legislature's intent. For instance, OCABR incorporated identical language from the Data Breach Law's Section 2(a) as its purpose clause, closely tying the *Standards* to its enabling legislation and eliminating numerous minor differences.

In at least one case, however, a new *Standards* definition clarifying the Holders covered by the regulation appears to expand OCABR's authority beyond the Data Breach Law's clear language. Originally, under Section 2(a) of the Data Breach Law, a Holder was "any person that owns or licenses personal information." Notably, none of the terms "owns," "licenses," "stores" or "maintains" were defined in either the Data Breach Law or the *Standards* until August 2009, when OCABR defined "owns or licenses" to encompass a variety of activities, including storing and maintaining Personal Information.<sup>80</sup>

The legislature's terminology is not so broad as the OCABR's; in fact, the legislature appears to differentiate between "owns or licenses" and "maintains or stores" in order to make an important distinction in M.G.L. ch. 93H, Section 3(a) (regarding notification requirements): a "person or agency that maintains or stores, but does not own or license data" need only notify and cooperate with the data's owner or licensor rather than complete the full notification process required of data owners/licensors. Thus, a person maintaining or storing Personal Information is held to a lesser standard than the owner/licensor – a distinction suggesting that the legislature, by its clear language, intended that the *Standards* be applied only to owners/licensors. In most cases, the August 2009 amendments appeared to move the *Standards* closer to their statutory predicate; however, OCABR authority has continued its expansion.

In addition, Section 5 of the Data Breach Law requires Holders to comply with "any applicable general or special law or federal law regarding the protection and privacy of personal information; provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter."<sup>81</sup> Noncompliance with such other laws returns the applicable person or agent to the Data Breach Law's requirements; under one law or another, the baseline requirement is that the Holder take appropriate responsive action. The language contained in the Data Breach Law represents the ordinary level of respect for other applicable law, albeit in a data breach situation. Its absence from the *Standards* suggests

---

<sup>80</sup> "Owns or licenses" now means: "receives, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment." As explained in the FAQ, this language clarifies that the *Standards* will not apply "to natural persons who are not in commerce." Limiting the *Standards* applicability to Holders providing "goods or services" or employment likely excludes few that would otherwise be Holders given the ordinary uses of Personal Information.

<sup>81</sup> Continuing, Section 5 relates responsive actions required upon a data breach, including notices to affected Massachusetts residents, the Attorney General and OCABR's undersecretary.

## LABOR & EMPLOYMENT ALERT

---

a further disconnect with the Data Breach Law.<sup>82</sup> Issues associated with multi-jurisdictional compliance are discussed above; the possibility that these problems arise from regulatory overreaching is yet another reason to proceed cautiously with extra-jurisdictional enforcement.

### **Impact Upon Holders and Their Business**

Holders should evaluate: (i) the Personal Information that they own, license, store or maintain; (ii) the state of their policies, procedures and systems; (iii) whether the *Standards* apply to them or their business; and (iv) whether the *Standards* apply to them by virtue of their business contacts with others (requiring Holder compliance to maintain the relationship). Even if a Holder believes the Massachusetts *Standards* do not apply in a particular situation, Holders should be aware of the national scope of the *Standards* and the general trend toward more heavy-handed regulation of personal information security.

Since the *Standards* provide affirmative obligations including, without limitation, WISP development and technical system security work, compliance will not be cheap. OCABR's impact statement estimated small business compliance costs to equal (for every ten employees) \$3,000 initially and \$500 per month afterward.<sup>83</sup> In arriving at this figure, OCABR made numerous, specific assumptions regarding small business, including: (i) types of Personal Information protections currently afforded by small business; (ii) available technologies and types of computer and other, equipment; and (iii) compensation rates and productivity of technical support personnel.<sup>84</sup> Because of these assumptions, affected parties must make their own respective budgetary projections and decisions regarding compliance preparations and follow-through.

### **Additional Government Guidance**

Additional OCABR guidance is available on its website, [www.mass.gov/ocabr](http://www.mass.gov/ocabr).<sup>85</sup> Guidance includes a link to frequently asked questions, public comments received by OCABR, and a transcript of the January 16, 2009 public hearing. Links to a "compliance checklist" and "model WISP" were disabled upon issuance of revised regulations in August 2009; OCABR is expected to update these links when new material becomes available. OCABR's old "model" program set forth some practical suggestions for implementation and was a useful tool; however, it also included provisions that exceeded the *Standards*' scope. Any updated model issued by OCABR will likely share similar strengths and weaknesses. Accordingly, Holders should use the model program as a guide only and should seek an attorney's advice to effectively adapt that model program to each Holder's particular circumstances.

### **Conclusion**

Although many from the business community originally questioned the *Standards*' prescriptive approach, even those commentators would count identity theft prevention and safeguarding Personal Information as worthy goals. Holders must recognize that they hold Personal Information in a fiduciary capacity – as part of a public trust – and adopt stronger data security practices. OCABR's recent amendments mark an

---

<sup>82</sup> *LIAM Letter*, at 1-2; *PCIAA Statement*, at 2.

<sup>83</sup> OCABR's *Fiscal Effect and Small Business Impact Statement*, [http://www.mass.gov/?pageID=ocaterminal&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca&b=terminalcontent&f=idtheft\\_sbimpact&csid=Eoca](http://www.mass.gov/?pageID=ocaterminal&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca&b=terminalcontent&f=idtheft_sbimpact&csid=Eoca). See also, *NFIB Testimony*, at 1.

<sup>84</sup> Though some have lauded OCABR's efforts in this regard, others have questioned the largely unscientific – and conservative – methodology employed in OCABR's fiscal impact statement.

<sup>85</sup> See also the direct link to OCABR's *Identity Theft* online services, <http://www.mass.gov/?pageID=ocatopic&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca>

## LABOR & EMPLOYMENT ALERT

---

adjustment to its regulatory approach. OCABR has issued regulations more in step with its enabling legislation, business community concerns and the public trust and has removed some obstacles to achieving the goals noted above. Though some *Standards* requirements have been softened, the deadline remains. Holders owning, licensing, receiving, maintaining, processing, or otherwise having access to Personal Information must work steadily toward *Standards* compliance on or before March 1, 2010.

*For more information, contact Michael C. Hackett at [mhackett@eckertseamans.com](mailto:mhackett@eckertseamans.com) or 617-342-6835. Mr. Hackett is a corporate attorney at Eckert Seamans Cherin & Mellott, LLC's Boston office practicing in the Business Division. In addition, you may contact any other Eckert Seamans Cherin & Mellott, LLC attorney with whom you have been working.*

NOTE: The information in this Alert is for general, educational purposes. It is not intended to be, and should not be considered, legal advice with respect to any particular situation.