**THE GLOBAL PRIVACY ALLIANCE**

# BREACH NOTIFICATION LEGISLATION KEY ELEMENTS TO CONSIDER[1]

## OVERVIEW

### *What is a Data Breach?*

A data breach generally refers to instances where personal information has been subject to unauthorized access, collection, use or disclosure. The data breach may be caused by inadvertent or deliberate actions that result in the information being stolen, lost or disclosed. For example, a breach may be a result of a deliberate theft of storage devices or infiltration (hacking) of computer systems by an unauthorized individual; alternatively, inadequate or sloppy data security practices may be to blame.

### *Notification about the Data Breach*

After a data breach occurs, the question that typically arises is whether the affected individuals and/or the relevant government authorities should be notified about the breach. Specifically, what types of breaches should trigger notification obligations and to whom? Moreover, if individuals and/or government authorities should be notified, when should such notification occur and what information about the data breach should be provided? A growing number of countries around the world have enacted or are considering enacting rules on data breach notification and the standards being adopted or considered vary widely.

### *Breach Notification Objectives.*

Breach notification obligations can serve important individual and public policy objectives. From the individual perspective, the primary purpose of notification is to enable individuals to mitigate the risk of identity theft or fraud when a breach occurs. In contrast, the primary purpose of government reporting is to enable the authorities to exercise their regulatory oversight functions, for example, to identify persistent or systemic security problems and take action as needed to address those problems. In addition, individual and public authority reporting obligations can serve to motivate organizations to implement more effective security measures to protect sensitive information.

### *Setting a National Standard.*

National uniformity is critical to providing consistent protection to individuals and to preserving a fully functioning and efficient national marketplace. Multiple local or provincial laws that impose a myriad of actual or potentially conflicting notification requirements do not serve the public interest but result in both higher costs and uneven individual protection. Rather, a

[1] The Global Privacy Alliance ("GPA") is comprised of a cross section of global businesses from the financial services, automobile, aerospace, consumer products, computer and computer software, communications, and electronic commerce sectors. The GPA works to encourage responsible, global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

national standard will avoid creating confusing and conflicting obligations and promote the public interest.

Lessons can be learned from the U.S. experience where the growing number of state laws has complicated the compliance obligations of organizations that operate in more than one state or more than one industry. For example, although a security breach may involve the same types of information about individuals in different states, the individuals may be entitled to receive different types of notices (or no notice at all), despite the fact that the harm they may suffer as a result of the breach is the same. In addition, the increasing array of obligations imposed on organizations has the potential to make it difficult for them to comply in one jurisdiction without running afoul of the obligations imposed on them in another.

Moreover, in light of the blurred boundaries of today's increasingly technological world, security breaches do not recognize provincial, or even national, boundaries. With respect to a security breach, the individual to whom the breached information relates may reside in one province, the criminal who caused the breach may reside in another province, the business victim of the breach may be located in a third province and the information may have been obtained in a fourth province. In this context, the security of information will be promoted most efficiently and effectively by a uniform national standard.

In light of the U.S. experience, a growing number of countries, such as France, Germany, Ireland, and the UK in Europe, Australia and New Zealand in the Asia-Pacific region, and Canada in North America, are developing or contemplating developing national standards to ensure that any breach notification regime that they may adopt does not result in a myriad of conflicting provincial laws. The European Union is also discussing the scope of possible Community-wide data breach notification obligations. At present, mandatory breach notification obligations at the national level exist only in Germany, Japan, the UAE, and the U.S.

## KEY ELEMENTS

### 1. Notification Trigger.

The goal of a notification law should be to define a reasonable and balanced notification trigger that ensures that individuals receive notice when there is a significant risk of substantial harm as a result of a security breach but that does not result in overnotifying and desensitizing individuals to these important notices. Moreover, because notification to individuals and public authorities serves different purposes, there should different notification triggers for both groups.

*Individuals.* The primary purpose of providing notices to individuals is to enable them to take steps to mitigate the risk of harm that might result from a breach. Thus, any individual notification requirement should be risk based. In this regard, notification should focus on two types of risk. First, with respect to sensitive financial information (discussed below), any notification requirement should be limited to situations where there is a "significant risk" that sensitive financial information compromised in a breach will be used to commit identity theft or to make fraudulent transactions using an individual's account. In addition, with respect to sensitive health information (also discussed below), any notification requirement should be limited to situations where there is "significant risk" that sensitive health information compromised in a breach will be used to cause the individual "significant harm," such as, for example, loss of business or employment opportunities because of an individual's health.

Although serious, many, if not most, security breaches do not result in significant harm to the individuals to whom the breached information relates. For example, in many cases, media containing data about individuals is simply lost or misdirected without involving any misuse of the data. In addition, businesses increasingly store and transmit customer data in a variety of unique media forms that require highly specialized and often proprietary technology to read, including sophisticated encryption. Thus, even if customer data finds its way into the wrong hands, the data often are not in a readable or usable form. Any notification requirement should recognize that the risks associated with each breach will differ and, as a result, the appropriate response to each breach also will differ.

Moreover, notification in the wake of each incident of data breach, without regard to the high risk of significant harm that might result, promises to have a counterproductive effect of overwhelming individuals with notices that bear no relation to the actual risks and, therefore, might not only needlessly frighten and confuse people, but also likely desensitize them and cause them to ignore the very notices that explain the action they need to take to protect themselves from harm when there is a significant risk.

*Public Authorities.* As stated above, the primary purpose of government reporting is to enable the authorities to identify persistent or systemic problems and take action as needed to address those problems. Given these objectives, it does not makes sense to establish requirements to notify government authorities about a security breach believed to affect only a few individuals (in addition to notifying the individuals themselves). Moreover, frequent reporting about relatively minor security breaches will overwhelm the public agencies responsible for consumer protection and data security regulation, whose resources are most likely already stretched thin. Consequently, only major breaches (*e.g.*, those affecting more than 10,000 individuals) should be reported. A threshold should be selected that is most appropriate for a country's market size. In addition, the public authority may also wish to require reporting whenever there has been a material privacy breach that involves suspected criminal activity outside the organization regardless of the number of individuals affected.

*Current International Approaches*

Australia. The Australian Law Reform Commission (the "ALRC"), was given the task by the government of conducting a comprehensive review of privacy regulation in Australia, and then issued a 1,983-page discussion paper[2] in September 2007 that proposed, among other things, that the Privacy Act be amended to include a breach notification obligation. In particular, the ALRC recommends that notification be triggered *"when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or the Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual."* The Office of the Privacy Commissioner (the "OPC") of Australia supports the higher notification threshold recommended by the ALRC because it believes that this approach would not require organizations to notify affected individuals or the Privacy Commissioner of less serious privacy breaches and would reduce the compliance burden on organizations relative to other approaches. The OPC also agrees that the Privacy Commissioner should be able to require notification where he or she believes that the unauthorized acquisition gives rise to a real risk of serious harm to any affected

[2] "Discussion Paper 72, Review of Australian Privacy Law" (DP 72, September 2007) is available at http://www.austlii.edu.au/au/other/alrc/publications/dp/72.

individual, even if the organization disagrees.[3] The government, however, has yet to formulate its response to the ALRC recommendations.

*Voluntary Guidelines.* In August 2008, the OPC issued advisory guidance on handling data breaches.[4] The guidance recommends notification to affected individuals if the breach creates a real risk of serious harm to the individual. Companies may decide for themselves whether to report the breach to the OPC but are essentially encouraged to report significant personal information security breaches to the Privacy Commissioner.

Canada. In the fall of 2007, the government launched a public consultation on breach notification in which it proposed that there be different notification thresholds for individuals and the authorities.[5] The government believes that notification to individuals should occur where there is a high risk of significant harm from the loss or theft of personal information. The Privacy Commissioner should be notified in the event of any major loss or theft of personal information within a specified time-frame to allow for oversight of organizational practices and enable the Privacy Commissioner to track the volume and nature of breaches, and the steps taken by organizations.[6] The government does not believe, however, that the Privacy Commissioner should have the responsibility to decide when notification should be given. In its view, the organization experiencing the breach is better positioned to understand and assess the risks involved and to make a prompt determination regarding whether and how to proceed with notification of its customers, business partners and/or the general public.[7] As of July 2009, no further action on this issue has been taken by the government.

*Voluntary Guidelines.* The Office of the Federal Privacy Commissioner issued voluntary breach notification guidelines in August 2007.[8] The OPC guidelines suggest that if a privacy breach creates *a risk of harm* to an individual, those affected should be notified. Each incident must be considered on a case-by-case basis to determine whether privacy breach notification is required. Organizations are also encouraged to inform the appropriate privacy commissioner(s) of material privacy breaches so they are aware of the breach. The key consideration in deciding whether to notify affected individuals should be whether notification is necessary to avoid or mitigate harm to that individual if his/her personal information has been inappropriately accessed, collected, used or disclosed. Organizations should also take into account the ability of the individual to take specific steps to mitigate any such harm. Other factors are to be evaluated when assessing whether to report a breach to the OPC (see below).

---

[3] The Office of the Privacy Commissioner's "Submission to the Australian Law Reform Commission's Review of Privacy – Discussion Paper 72," issued in December 2007, is available at http://www.privacy.gov.au/publications/alrc211207.html.

[4] *See* Guide to handling personal information security breaches (August 2008), available at http://www.privacy.gov.au/business/guidelines/index.html.

[5] *See* "Implementation Of The Government Response To The Fourth Report Of The Standing Committee On Access To Information, Privacy And Ethics On The Personal Information Protection And Electronic Documents Act," available at http://canadagazette.gc.ca/partI/2007/20071027/html/notice-e.html#i2.

[6] The Canadian government has yet to define what should constitute a major breach that would trigger government reporting obligations.

[7] *See* "The Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics," available at http://www.ic.gc.ca/epic/site/ic1.nsf/en/00317e.html.

[8] See "Key Steps for Organizations in Responding to Privacy Breaches," available at http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp.

Germany. In July 2009, the Federal Data Protection Act was amended to include data breach notification requirements.[9] The provision, which will enter into force in September 2009, will require private-sector businesses and certain federal state agencies (e.g., public electricity providers) to give notice in cases where any of the following sets of data are leaked: sensitive data, criminal records, bank account or credit card data, or personal data subject to legal privilege (e.g., data held by lawyers, doctors, journalists, etc.). The proposed rules only require notification for leakages that may lead to "serious impediments for privacy and other individual interests." The types of data, as well as the possible results of the breach (e.g., damages or identity theft), must be taken into account when determining whether such "serious impediments" exist. Both the data protection authority and all affected individuals must be notified "immediately" (as soon as reasonably possible) after containment.

Ireland. Interim guidelines published by the Irish Data Protection Commissioner in April 2009[10] recommend that organizations notify the Office of the Data Protection Commissioner of all data breaches involving unauthorized or accidental disclosures of customer or employee personal information. The DPA has adopted this voluntary approach while the Minister for Justice, Equality & Law Reform carries out a review of this issue to determine whether breach notification should be made mandatory.

Japan. The ministerial guidelines issued immediately after the enactment of the Personal Information Protection Law recommended, and in some cases required, that notification be given to individuals and government authorities every time a breach occurred relating to any personal information. As a result, organizations began to notify the public and the relevant ministry of every security breach, regardless of the size of the breach, the nature of the personal information involved or the risk of misuse of the information. Notices that bore no relation to the actual risks posed by the breach served to frighten and confuse people as well as desensitize them to future notices where they might need to take steps to protect themselves from harm. In response to this experience, Japan's Ministry of Economy, Trade and Industry ("METI") revised its guidelines and, among other things, established different notification triggers for notifying individuals.[11] Organizations now do not have to provide notice about breaches to individuals when their rights and interests have not been or are not likely to be infringed by the data breach. For example, notice does not need to be provided to the individual when: 1) personal data that has been lost is recovered immediately without being seen by a third party; 2) advanced encryption is used to protect the data; and/or 3) the organization responsible for the breach is the only one capable of identifying the specific individual (by collating it with personal data that only the organization retains). The Financial Services Agency ("FSA"), however, still requires under its guidelines that individuals be notified about all breaches, even if the data have been encrypted using advanced techniques. Under both the METI and FSA guidelines, government authorities are to be notified about all data breaches, regardless of the size or severity; although METI permits organizations to report breaches to either the government authorities or the approved personal information protection group[12]. In addition, a public announcement must be made to prevent any

[9] *See* Section 42a of the Federal Data Protection Act. Available (in German) at http://dip21.bundestag.de/dip21/btd/16/120/1612011.pdf.
[10] See "Breach Notification Guidance," available at http://www.dataprotection.ie/viewdoc.asp?DocID=901&ad=1.
[11] The METI Guidelines use the term "preferable" to refer to actions that are not required, but that businesses should make their best effort to observe. In contrast, breach notification is mandatory under the FSA Guidelines.
[12] Approved Personal Information Protection Organizations ("APIPO") are organizations in the Japanese private sector which have received approval from the Competent Minister to resolve disputes regarding the handling of

secondary damage that might result from the breach; however, METI does not require a public announcement if all affected persons have been notified individually, the personal data was immediately recovered without being seen by a third party; and advanced encryption was used to protect the data and the business responsible for the breach is the only one capable of identifying the specific individual (by collating it with personal data that only the business retains).

New Zealand. In February 2008, the New Zealand Privacy Commissioner issued voluntary breach notification guidelines modeled on the Canadian OPC approach.[13] The guidelines recommend that individuals should be notified when there is *a foreseeable risk of harm*. In addition, organizations are encouraged to report *material privacy breaches* to the Office of the Privacy Commissioner.

UAE. Under the data protection law of the Dubai International Financial Centre (the "DIFC"), the data controller or data processor must inform the Commissioner of Data Protection of *any unauthorized intrusion* as soon as reasonably practicable. There is no obligation to notify affected individuals.

United Kingdom. In March 2008, the U.K. Information Commissioner's Office (ICO) released non-binding guidance on how organizations should manage a data security breach and when to notify the ICO of such breaches.[14] The Information Commissioner recommends that "serious" breaches should be brought to the attention of the ICO. The hallmarks of a serious breach include the potential for harm to data subjects, the number of individuals affected by the breach, and the sensitivity of the breached data. The ICO said an example of the potential for harm caused by a breach is the loss of financial information.

United States. More than 40 states in the U.S. have enacted laws imposing notification obligations on organizations that discover, or are themselves notified about, a breach of security of their information systems. In general, state security breach notification laws are understood to be modeled on the California law, which went into effect on July 1, 2003 (the "California Law").[15] Most of these states require organizations to notify individuals of a breach of security in which certain personal information relating to those individuals was or is reasonably believed to have been acquired by an unauthorized person. Several state notification laws, however, also impose notification obligations based upon a determination that the acquisition creates an elevated degree of risk of harm to an individual, such as a risk of identity theft or other fraud that could be committed against the individual. For example, Florida law includes a notification trigger that provides that the acquisition must be *unlawful* or unauthorized and must *materially compromise* the security, confidentiality or integrity of the information. [16] North Carolina and

---

personal information by subject businesses pursuant to Art. 37 of the Personal Information Protection Law, as well as provide information to subject businesses. APIPO may be notified in lieu of the government authorities, except when the breach involves sensitive information (credit card numbers, religious, political, race, sex, health information, etc.) or a repeat offender.

[13] *See* Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist, available at: http://www.privacy.org.nz/privacy-breach-guidelines-2/

[14] *See* Guidance on data security breach management and Notification of Data Security Breaches to the Information Commissioner's Office, available at: http://www.ico.gov.uk/what_we_cover/data_protection/guidance/good_practice_notes.aspx.

[15] Cal. Civ. Code § 1798.82 (LEXIS through 2007, ch. 12, June 7, 2007).

[16] Fla. Stat. §§ 817.5681(1)(a), (4).

Ohio laws specifically provide that notification is triggered if the breach creates a *material risk of harm* to a consumer. [17]

With respect to reporting to public authorities, several states, including Hawaii, Louisiana, Maine, Maryland, New Hampshire, New Jersey, New York and North Carolina, as well as Puerto Rico, have prescribed requirements to notify specified state authorities about any breach of security. Under the Louisiana notification law, for example, a regulation adopted by the State Attorney General's office requires an entity to provide a written notice detailing the breach of security, including the names of affected Louisiana citizens, to the Consumer Protection Section of the Attorney General's office within 10 days of distributing notices to Louisiana citizens.[18] The New Jersey law requires a company to notify that state's Division of State Policy *prior to* notifying a customer who resides in New Jersey.[19]

**2. Definition of Specified Personal Information.**

Legislation imposing notification obligations should specify the sensitive information that would be subject to these obligations. Specifically, notification should be based on the types of information that could be used to cause the "significant harm" that the notification requirement is designed to help individuals mitigate. With respect to a risk of identity theft or financial fraud, the notification obligation should be limited to identifiable and unencrypted data that includes an individual's name together with one or more sensitive data elements, such as a national identification number (or other number that can be used to open a financial account) or financial account information together with any password or pin number that can be used to access the underlying account. With respect to a risk of substantial harm from the misuse of health information, the notification obligation should be limited to identifiable and unencrypted data that include an individual's name together with one or more sensitive health data elements, such as a social security number or government identification number or health information, such as, for example, a medical diagnosis ("Specified Personal Information").

In doing so, organizations can both work proactively to strengthen safeguards for this Specified Personal Information and, if various security breach incidents do occur, focus their responses on those incidents that relate to this information. Data that have been de-identified, encrypted or otherwise adequately secured (using other technology), however, should not be covered because an incident affecting such data does not pose a high risk of significant harm to individuals. Moreover, if the breach involves data that are publicly available, such data elements should be excluded from the risk analysis.

*Current International Approaches*

Australia. There appears to be a consensus that specified information should not include encrypted data. There is no consensus yet on the specific data elements that should be included. The voluntary guidelines simply advise that some information such as health information, government identifiers, and financial account numbers may be more likely to cause individual harm. In addition, a combination of personal information is considered to create a greater risk of harm than a single piece of information. Furthermore, the sensitivity of the information, the context of involving the affected information, and/or how the information could be useful (e.g.,

[17] N.C. Gen. Stat. § 75-65(a); Ohio Rev. Code Ann. § 1349.19(B)(1).
[18] 33 La. Reg. 466.
[19] N.J. Stat. § 56:8-163c(1).

for fraudulent or harmful purposes) should also be considered when deciding whether or not notification may be required.

Canada. The government has not yet put forward its views on the specific data elements that should be included; however, in the OPC guidelines, the Privacy Commissioner advised organizations to look at what data elements have been breached, the sensitivity of the information, the context of the personal information involved, whether the data are adequately encrypted, anonymized or not otherwise easily accessible, and how the information can be used. The guidelines noted that a combination of personal information is typically more sensitive than a single piece of personal information and that combinations of certain types of Specified Personal Information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.

Germany. Notification must be given when the breach involves sensitive data (e.g., data concerning health or sex life, racial or ethnic origin, political opinions, religious beliefs), criminal records, bank account or credit card data, or personal data that is subject to legal privilege (e.g., data held by lawyers, doctors, journalists, etc.).

Ireland. Under the voluntary guidelines, the Office of the Data Protection Commissioner should be notified about breaches involving any personal information.

Japan. Loss of any personal data can potentially trigger notification obligations; however, the METI guidelines do provide exceptions for encrypted data while the FSA guidelines do not.

New Zealand. The voluntary guidelines recommend that organizations consider the sensitivity and context of the information involved in the breach and/or how the information could be used (e.g., for fraudulent or harmful purposes). In addition, a combination of personal information is considered to create a greater risk of harm than a single piece of information.

UAE. The DIFC law does not distinguish among the data elements. Any breach of personal information requires notification to the authorities.

United Kingdom. While the ICO guidance does not specify the data elements that would trigger notification, it notes that there is likely to be a significant risk of substantial harm when sensitive personal data are involved.

United States. The California Law defines "personal information" as an individual's first name or initial and last name in combination with one or more "data elements," if either the name or the data elements are not encrypted. These data elements are:

- Social security number (SSN);
- Driver's license or state identification card number; or
- Account, credit card or debit card number in combination with any required security code or password that would permit access to an individual's financial account.

Many state notification laws define "personal information" in similar terms; however, several laws provide that only the data elements that need to be encrypted, redacted or secured by another method rendering the element unreadable or unusable be considered "personal information."

Several state notification laws have expanded the scope of personal information to include different types of data elements such as medical information, biometric data and fingerprints. In addition, many of these state laws follow the California Law by providing an exception for certain types of information "available to the general public." A few state laws also apply to a breach of security affecting *paper records* containing personal information, as opposed to electronic records.

**3. Risk Determination.**

A determination of whether a particular incident affecting identifiable, unencrypted Specified Personal Information poses a risk of significant harm to the individual should be based on an assessment of the circumstances surrounding the incident. In particular, the following factors should be considered when assessing the potential risk to the individual or organization:

- The Causes of the Breach. If there has been an incident affecting identifiable or unencrypted Specified Personal Information, then the next step will be to assess the nature and extent of the incident, including the number and nature of unauthorized recipients, whether the Specified Personal Information was lost or stolen and, if stolen, whether the Specified Personal Information was specifically targeted for theft. In addition, consideration should be given to the steps taken by the organization to minimize the harm and whether the incident appears to be isolated or part of a pattern of systematic efforts to obtain information.

- Potential for High Risk of Significant Harm. Organizations would also need to determine the type of harm to individuals that could result from the breach (*e.g.*, security risk/risk to physical safety, identity theft, financial loss, loss of business or employment opportunities), how a potentially affected individual is likely to perceive the potential risk and whether an individual can take any steps to reduce this risk.

Based on an assessment of these factors, organizations should determine whether or not a given incident poses a risk of significant harm to individuals, thereby triggering notification obligations. If an organization determines that there is a risk of significant harm, it will then need to determine when and how to notify affected individuals, as well as potentially providing notice to the public authorities about a major breach.

*Current International Approaches*

Australia/Canada/New Zealand/United Kingdom. The Privacy Commissioners' guidelines are in line with the above approach.

Ireland/Japan/UAE. The issue of risk assessment is not addressed.

Germany. The types of data, as well as the possible results of the breach (e.g., damages or identity theft), must be taken into account when determining whether such "serious impediments" exist.

United States. The California Law provides that covered entities must disclose a "breach of the security of the system" (defined as an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the

person or business) when unencrypted personal information is reasonably believed to have been *acquired* by an unauthorized person.[20] Under the California Law, a company should evaluate whether the breach has *compromised*, or is reasonably likely to *compromise*, the security, confidentiality or integrity of the information and, if so, notify potentially affected individuals accordingly. Many other state laws prescribe a standard for notifying individuals that is substantially similar to the standard under the California Law.

Several other states provide that a covered entity shall, when it becomes aware of a breach of the security of the system, conduct a prompt investigation in good faith to determine the likelihood that personal information has been or will be misused. Notice must be made unless the investigation determines that the misuse of information has not occurred and is not reasonably likely to occur. For example, the Maryland and Maine laws impose notification duties based on this standard.[21]

**4. Timing and Method of Notification.**

*Individuals*. While notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the scope and nature of the breach, remedying any ongoing breach and identifying the potentially affected individuals, the law should permit notification to be delayed at the request of a law enforcement agency in order to carry out its own investigation. For example, before notification is provided and before a breach is publicized in the media, law enforcement will have a better opportunity to catch the culprits involved (thereby, preventing future breaches from occurring or mitigating the harm felt by individuals).

The law should be flexible with respect to the method of notification. The most important feature should be to get notice to affected individuals. The method used should depend on the particular circumstances surrounding the organization's relationship, if any, to the potentially affected individuals, the manner in which the organization typically communicates with them and the type and scope of the breach. For example, some organizations, such as banks, regularly mail monthly statements to account holders. Consequently, postal mail notification may be the most logical choice for these organizations. Alternatively, other organizations may rely more on their websites as their means to communicate with their customers and potential customers and, therefore, should be permitted to use electronic methods to notify individuals. In addition, website notification or other methods of mass communication may be more appropriate when a breach involves large numbers of individuals (*e.g.*, 1,000-250,000 individuals).

Consequently, organizations should be permitted to select the most appropriate method of communication, taking into account the way in which the organization typically communicates with individuals and the circumstances surrounding a given breach. Acceptable methods of communication should, therefore, include direct notice by postal mail, e-mail, telephone, or face-to-face communications, or through generally accessible notification methods (*e.g.*, website information, posted notices or mass media). Mass communications may be appropriate if direct notification is likely to cause further harm, is prohibitive in cost or the contact information for potentially affected individuals is not known. Moreover, using multiple methods of notification

[20]Cal. Civ. Code §§ 1798.82(a) and (d).

[21]Colo. Rev. Stat. § 6-1-716(2)(a); Del. Code Ann. tit. 6, § 102(a); Idaho Code Ann. § 28-51-105(1); Kan. Stat. Ann. § 50-7a02(a); Neb. Rev. Stat. Ann. § 87-803(1); N.H. Rev. Stat. Ann. § 359-C:20(I)(a); SB 194 (Md. 2007), to be codified at Md. Code Ann., Com. Law § 14-3504(B); Me. Rev. Stat. Ann. tit. 10, § 1348(1)(A).

in the same security incident depending on the relationship with the individual in certain cases may also be appropriate.

*Public Authorities.* As discussed earlier, only major breaches should be reported to the authorities. Frequent government reporting about relatively minor security breaches will overwhelm the agencies responsible for consumer protection and data security regulation. The method of notification should reflect the specific needs of the public authority, but should not be so burdensome as to cause delay in notifying individuals.

*Current International Approaches*

Australia. Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. If law enforcement authorities are involved, organizations should check with those authorities whether notification should be delayed to ensure the investigation is not compromised. Direct notification (e.g., telephone, letter, email or in-person) is preferred; indirect notification (e.g., website information, posted notices, media) should generally only occur when direct notification would cause further harm. Organizations are encouraged to report significant personal information security breaches to the Privacy Commissioner.

Canada. The Privacy Commissioner's guidelines recommend that notification of affected individuals occur as soon as reasonably possible following assessment and evaluation of the breach, unless a delay is warranted to ensure that the investigation is not compromised. The preferred method of notification is direct – by phone, letter, e-mail or in person – to affected individuals. The Privacy Commissioner believes that indirect notification – website information, posted notices or mass media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, or the contact information for affected individuals is not known. Using multiple methods of notification in certain cases may be appropriate. Organizations should also consider whether the method or level of detail of notification might increase the risk of harm (*e.g.,* by alerting the person who stole the laptop of the value of the information on the computer). In addition, the organization that has a direct relationship with the customer, client or employee typically should be the one to notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information. However, there may be circumstances where notification by a third party is more appropriate.

Germany. Individuals and government authorities must be notified "immediately" (as soon as reasonably possible) after containment. In cases where a large public is affected, public announcements in at least two national newspapers may replace individual notices. These announcements must be at least half a page long. The notice should include information on the data leakage, possible results of the leakage as well as measures being taken to mitigate damages.

Ireland. The guidelines recommend that organizations notify the Office of the Data Protection Commissioner as soon as they become aware of unauthorized or accidental disclosures of customer or employee personal information. The Office of the Data Protection Commissioner will then discuss with the organization whether notice to the affected persons should be given (if the organization has not already done so) and how such notice should be provided.

Japan. The FSA requires that notice regarding the relevant facts of the breach be given to individuals "promptly." In addition, notice to the competent minister(s) must be given immediately and a public announcement must be made promptly regarding the relevant facts of the breach and measures taken to prevent further breach to prevent further incidents. In contrast, the METI guidelines do not specify a specific timeframe for notification except in cases of breaches involving sensitive data. When sensitive data is involved, reports must be made immediately when: 1) the breach involves sensitive information, credit information and credit card number and there is a likelihood that secondary damage will happen; 2) when there are repeated breaches of the same company; or 3) when the APIPO decides that such reporting is necessary.

New Zealand. Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. If law enforcement authorities are involved, organizations should check with those authorities whether notification should be delayed to ensure the investigation is not compromised. Direct notification is preferred; indirect notification should generally only occur when direct notification would cause further harm.

UAE. The data controller or data processor must inform the Commissioner of Data Protection of *any unauthorized intrusion* as soon as reasonably practicable. There is no obligation to notify affected individuals.

United Kingdom. The ICO guidance does not specify a timeframe for notifying affected individuals and/or government authorities or the method of notification.

United States. Under the California Law, a company must disclose a breach to potentially affected individuals "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. Many states have adopted substantially similar language. In addition, several state laws also provide a delay if notification may jeopardize national security.

With respect to the method of notification, notice to individuals may be provided under the California Law by written notice, electronic notice or "substitute notice."[22] Most state security breach notification laws contain similar provisions regarding the methods of notifying individuals about a breach, although some states specify, for example, that electronic notice may be used only if the person's primary means of communication with the individual is by electronic means, while others also allow telephonic notice.

Under the California Law, substitute notice may be used if the person or business demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000 or the person or business does not have sufficient contact information. The majority of states have adopted this language but in some cases have

[22] Substitute notice involves the following three actions: (1) e-mail notice when the company has e-mail addresses for the subject persons; (2) conspicuous posting of the notice on the company's web page, if it maintains one; and (3) notification in a major statewide medium.

established different thresholds for the costs of notification or the population of individuals who are potentially affected by the breach.

Lastly, with respect to government reporting, several states, including Hawaii, Louisiana, Maine, Maryland, New Hampshire, New Jersey, New York and North Carolina, as well as Puerto Rico, have prescribed requirements to notify specified state authorities about breaches of security. Under the Louisiana notification law, for example, a regulation adopted by that state's Attorney General's office requires an entity to provide a written notice detailing the breach of security, including the names of affected Louisiana citizens, to the Consumer Protection Section of the Attorney General's office within 10 days of distributing notices to Louisiana citizens.[23] The New Jersey law requires a company to notify that state's Division of State Policy *prior to* notifying a customer who resides in New Jersey.[24]

* * * * *

If you have any questions, please contact Miriam Wugmeister at 212.506.7213 or at mwugmeister@mofo.com.

[23] 33 La. Reg. 466.
[24] N.J. Stat. §§ 56:8-163c(1).