A Practice Note discussing certain US federal and state data breach notification laws relating to personal information and providing guidance on how to prepare for and respond to data security breaches.

This Note discusses US federal and state laws that require notification in the event of a data security breach involving personal information and provides practical tips on how to prepare for and respond to a data breach. In particular, this Note considers key issues relating to:

- State data breach notification laws.
- Federal data breach notification laws.
- Preparing for and responding to a data breach.

According to the Privacy Rights Clearinghouse's Chronology of Data Breaches, thousands of known data breaches in the US have compromised nearly 900 million records of individuals since 2005. Data breaches happen for many different reasons, including:

- Human error and accidents, such as:
  - losing a laptop or data storage device;
  - coding errors or system vulnerabilities that result in data publicly accessible on a website; or
  - misdirected communications.
- Illegal or malicious activity of individuals and criminal enterprises (whether employees or other insiders or unrelated third parties) through:
  - hacking into a business's computer system;
  - downloading or stealing records; or
  - obtaining information by pretext or theft of equipment.

The cost of a data breach can be significant in terms of both expense and reputation, including the actual cost of responding to the breach, lost business revenue and exposure to government fines and penalties as well as private lawsuits (see Box, Costs of a Data Breach).

No matter how robust a business's data security practices and policies, there is no way to ensure that a data breach will not occur and nearly all businesses already have or will likely suffer a breach incident at some point. Not responding appropriately can magnify the costs and other negative impacts of a data breach. Accordingly, companies should prepare for a data breach and develop a response plan that complies with legal obligations and reflects operational realities (see Preparing for and Responding to a Data Security Breach). The response plan should set out each step to take once a business suspects a breach has occurred.

Ensuring that all notifications are timely and include necessary content is crucial and requires knowledge of each relevant state and federal law. This Note does not cover every requirement of the state data breach notification laws. Businesses should consult with counsel in the event they suspect they have suffered a potential breach incident.

**STATE DATA BREACH NOTIFICATION LAWS**

Most states (plus the District of Columbia, Guam, Puerto Rico and the US Virgin Islands) currently have adopted data breach notification statutes. Only Alabama, New Mexico and South Dakota have not. These statutes require businesses to take certain steps when a data breach involving protected personal information occurs. Many states, including Florida and California, have separate provisions or statutes that apply to state agencies that suffer a data breach. Several states have enacted sector-specific laws in addition to their general data breach notification statutes. This Note focuses on general data breach notification statutes applicable to businesses.

California was the first state to adopt a breach notification statute and has since amended it four times. Most other state laws are modeled on or are substantially similar to California’s law as originally enacted. While similarities exist, there are many differences among the statutes.
Breach Notification

This Note addresses notification requirements generally, while pointing out some of the key variations among the statutes. Practitioners must be aware of the many variations in the laws of each state where an affected individual resides, including various sector-specific laws, when counseling clients affected by a multi-jurisdictional breach. The variations in the laws can have a greater or lesser impact depending on the facts of a given incident.

The National Conference of State Legislatures maintains a list of State Security Breach Notification Laws with links to the text of each law.

TRIGGERING THE BREACH NOTIFICATION REQUIREMENT

Most state breach notification statutes apply to only electronic records. However, a number of jurisdictions’ laws also apply to a breach of paper records. State data breach notification statutes may require notification of a breach, depending on the jurisdiction and circumstances, to:
- Affected persons.
- Law enforcement.
- State regulators.
- The media.
- Consumer reporting agencies.

Unauthorized Access or Acquisition

As a general matter, statutory breach notification obligations are potentially triggered when the security, confidentiality or integrity of an individual’s covered personal information has been compromised by either or both the actual or reasonable belief of an:
- Unauthorized access to data.
- Unauthorized acquisition of data.

Except for Connecticut and Mississippi, under the statutes, a good faith acquisition of personal information by an employee of the business, even if unauthorized, does not trigger notification provided the personal information is not used or subject to further unauthorized disclosure.

New York and Vermont, by statute, and other states, such as California, through informal guidance, provide non-exhaustive factors to help guide this determination, including assessing whether the information:
- Is in the physical possession or control of an unauthorized third party (including lost or stolen computers and devices).
- Has been downloaded or copied.
- Has been subject to unauthorized use.
- Has been made public.

Risk of Harm Thresholds

The majority of statutes include some type of risk of harm of threshold before notification obligations are triggered. The specific statutory language may vary, however, such as whether:
- The risk must be “substantial” versus “material.”
- Misuse is likely to occur or whether the business must affirmatively conclude that misuse is not likely.

These differences, while seemingly marginal, can be important. A few statutes require businesses to consult with law enforcement or notify the attorney general or another state agency before or if it determines notification is not required because there is no reasonable likelihood of harm.

Effect of Encryption or Other Means of Making Information Unusable

Most statutes provide that notification is not required if the personal information is encrypted. Some statutes further provide that encryption is not sufficient if the encryption key is also breached. Some other statutes also specify that notification is not required if the personal information is redacted, truncated or secured by another means, such that it is unreadable or unusable. The language of these provisions varies significantly.

Definition of Personal Information

Typically, state laws define personal information as an individual’s first name or initial with last name (and in some cases other identifiers) and one or more of the following data elements, unless either element is encrypted or (in some cases) otherwise made unreadable:
- Social Security number.
- Driver’s license number or state or military identification card number.
- Financial account, credit card or debit card number in combination with any required security code, access code or password that permits access to an individual’s account.

However, some states define personal information more broadly to include:
- Medical information.
- Health insurance information.
- A user name or email address, in combination with a password or security question and answer that permits access to an online or financial account or resource.

Some states also have expanded the definition of personal information to include one or more of the following:
- Date of birth.
- Mother’s maiden name.
- Biometric or DNA data.
- Passport number.
- Tribal identification numbers.
- Taxpayer identification numbers.
- Financial account numbers disassociated from passwords or pin numbers.
- Other information sufficient to commit identity theft.

Personal information generally does not include information that is legally, publicly available, although under some laws only if publicly available from government records.
NOTIFICATION REQUIREMENTS

Timing of Notice to Affected Individuals

Most statutes do not provide a set time for notification but rather require that the business notify affected persons as expeditiously as possible or practicable, without unreasonable delay or both. Some statutes define narrow circumstances that may serve as a premise for reasonable delay. For example, most statutes explicitly provide that the business may delay notification if law enforcement determines notice may impede a criminal investigation.

However, some statutes do contain specific timing requirements for notification to individuals. For instance:

- Florida requires that notification of individuals occur no later than 30 days from the determination of a breach, though a 15-day extension period is available under limited circumstances.
- Ohio and Wisconsin require notification within 45 days from the determination of a breach.
- In Maine, if the business delays individual notifications because of a law enforcement investigation, it must provide notification to individuals within seven business days after law enforcement determines that notification will not compromise a criminal investigation.

Significantly, several statutes require that entities notify state law enforcement or regulators before or at the time of notification of individuals (see Notice to Government Entities and Credit Reporting Agencies).

Form of Notice

For all states, notice in writing satisfies the notification requirement. Most states require written notice except in limited circumstances. While a few states broadly allow notice by email, most states do not allow email or other electronic notice unless it is provided under certain laws governing electronic notice. This effectively means that the business must have the affected individuals’ prior consent to provide email notice of the security breach in most states.

California’s statute, on the other hand, includes unique provisions allowing email notice when the breach involves a user name or email address with a password or security question and answer that would permit access to an online account and no other personal information covered by the law. Other requirements apply under the California statute where the breach involves email account login credentials furnished by the business.

In some circumstances, substitute notice is an option. Substitute notice may be permitted, for example, if:

- The business must notify a threshold number of individuals.
- The cost to notify exceeds a certain threshold.
- The notifying entity does not have sufficient contact information.

Substitute notice typically consists of one or a combination of the following methods:

- Notification by email when the notifying entity has email addresses for the affected individuals.
- Notice to or publication in the media.
- Conspicuous posting on the notifying entity’s website.

Contents of Notice

While many states do not require specific content in the notice to individuals, several do. Some of the requirements conflict, which creates expense and administrative burdens for a business experiencing a large data breach.

As a general matter, states with content requirements typically provide that notification include one or more of the following:

- The date of the notice.
- A description of the incident.
- The date or date range of the breach.
- A description of the actions the business is taking to contain or remedy the breach.
- The type of personal information affected.
- Whether notification was delayed due to a law enforcement investigation.
- Contact information for:
  - the notifying entity (with varying levels of specificity);
  - national consumer reporting agencies;
  - the Federal Trade Commission (FTC); or
  - the state attorney general’s office.
- Advice to the consumer to be vigilant and on how to protect themselves from fraud.

However, Massachusetts law specifies that the notice not include the nature of the breach. Massachusetts also requires specific details on how individuals can place a security freeze with the three nationwide consumer reporting agencies under Massachusetts law. This too requires tailored content and stands in contrast to other states with laws requiring that information about credit freezes and how to place them be provided, but which allows for a more general description such that the content can also be used for notices to other states’ residents.

Notice to Government Entities and Consumer Reporting Agencies

Many states also require notice to the state attorney general or some other state agency. Several states also require notice to the three major credit reporting agencies when a certain number of state residents are affected.

In some cases, a minimum number of affected residents triggers the requirement to notify state government entities. For example:

- California requires notification to the attorney general when more than 500 California residents will be notified.
- South Carolina requires notification to the Department of Consumer Affairs if more than 1,000 South Carolina residents will be notified.
- Florida requires notification to the Department of Legal Affairs if more than 500 people in Florida will be notified.

Hawaii, Missouri and Virginia include similar numerical thresholds.
Some states require this notification at the time of or before notifying affected individuals. Reporting to some states is done by submitting a specific form, as with New York, and frequently the law requires the business to also submit a copy of the notice letter to affected persons and report the number of affected residents. Other states require notice to certain state agencies within a specific time frame either from when the breach occurs or after individual notice.

For more information on the requirements for notice to state agencies, see State Agency Notice Requirements for Data Breaches Chart (http://us.practicallaw.com/5-501-9110).

Third-party Service Providers
State data breach laws typically distinguish between those parties who own or license the data that has been breached and third parties who have data in their possession, such as vendors. Laws typically require a non-data owner experiencing a breach of personal information to notify the data owner immediately following discovery or as soon as practicable. Florida, however, requires that the third party provide notice no later than ten days after discovery of the breach. Once the third party notifies the data owner, it is the data owner's responsibility to notify, or ensure notification of, affected individuals.

LIABILITY FOR FAILURE TO COMPLY
Most jurisdictions allow for enforcement by the state's attorney general or consumer protection agency, which typically can sue for civil or injunctive relief. Some data breach statutes cross-reference to other consumer protection statutes and penalties while other data breach statutes provide for specific remedies.

A significant minority of states, including California, Texas and New Jersey, include a private right of action that allows individuals to sue for actual damages resulting from an entity's failure to provide timely notice of a breach.

COMMON EXCEPTIONS AND OTHER GUIDANCE
Counsel should be aware that, especially for certain sector-specific businesses, statutory exceptions or other regulations or guidance may apply.

For example, several statutes include exemptions for:
- Health Insurance Portability and Accountability Act (HIPAA) covered entities.
- Financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) (see Federal Data Breach Notification Laws).

The specifics of these exemptions can vary significantly from state to state and may turn on whether the institutions are subject to specific federal regulatory guidance or are notifying affected persons under those regimes.

Businesses in certain sectors also may be subject to other state requirements or guidance. For example, several states, including California, Connecticut, Maine, New Hampshire, Oregon and Washington, have rules or guidance applicable to regulated insurance licensees and these rules sometimes include provisions requiring that notice also be made to the state insurance commissioner.

FEDERAL DATA BREACH NOTIFICATION LAWS
There is no single federal breach notification law. Rather, there are several sectoral laws that include notification obligations. These laws do not preempt state notification laws. Notable examples include:
- The GLBA (see GLBA).
- The HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) (see HIPAA and HITECH).

For an overview of additional federal privacy and data security laws, see Practice Note, Privacy and Data Security: Overview (http://us.practicallaw.com/6-501-4555).

GLBA
GLBA regulates the privacy and data security practices of financial institutions. In 2005, the federal banking regulators, which include the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC) and the Office of Thrift Supervision (OTS) (now part of the OCC), issued Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Interagency Guidance) (12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D-2 and part 225, app. F (FRB); 12 CFR part 364, app. B (FDIC); 12 CFR part 570, app. B (OTS)).

The Interagency Guidance provides that entities must:
- Investigate breaches when misuse of sensitive customer information has occurred or is reasonably possible.
- Notify their functional regulators and provide consumer notice if warranted.

Sensitive customer information includes a customer's name, address or telephone number, in conjunction with any of the following:
- Social Security number.
- Driver's license number.
- Financial account, credit or debit card number.
- A personal identification number or password that would permit access to the customer's account.

The Interagency Guidance is not limited to computerized data.

HIPAA AND HITECH
HITEA and HITECH apply to protected health information. The Department of Health and Human Services (HHS) issued final regulations in 2013 for HIPAA covered entities setting out the parameters for notifying individuals of data breaches involving unsecured protected health information. Protected health information is defined differently than personal information under most state statutes, which often limit notification to types of information more typically associated with the risk of identity theft. Therefore, HIPAA may sometimes require notification where state law would not require it. Key distinctions from state law include:
- Notification to individuals must occur within 60 days, subject to delays for law enforcement purposes.
The covered entity must notify HHS of the breach.

If the breach affects more than 500 individuals total, the covered entity must typically provide its notification to HHS contemporaneously with the notice to individuals.

If the breach affects more than 500 individuals in one state, the covered entity must notify prominent media outlets in the relevant state or jurisdiction.

In 2009, the FTC issued similar breach notification rules for certain entities that are not covered by HIPAA but that handle or interact with personal health records (for example, records contained in certain personal health apps).

For more information on the HITECH Act’s breach notification requirements, see Practice Note, HIPAA Breach Notification Rules (http://us.practicallaw.com/1-532-2085).

THE FCC CPNI BREACH RULE
The FCC has a data breach rule applicable to telecommunications carriers when they experience a breach of certain phone record information. A breach involves intentional and unauthorized access to, use or disclosure of CPNI. The rule includes a requirement that telecommunications carriers notify federal law enforcement and affected individuals.

PREPARING FOR AND RESPONDING TO A DATA SECURITY BREACH
While creating an information security program is outside the scope of this Note, vital components of preparing for a data breach include:

- Adopting strong policies and procedures for the collection, use, storage and disposal of personal information.
- Preparing a personal information inventory.
- Adopting an incident response plan.
- Testing the incident response plan.
- Training personnel on the incident response plan.

Understanding the nature and location of personal information that a business collects, stores and uses is crucial to understanding whether a breach has occurred, determining its scope and acting quickly when it is discovered. Businesses should evaluate carefully whether they are collecting and maintaining more personal information than necessary to minimize exposure in the event of a security incident.

For more information on creating an information security program, see Common Gaps in Information Security Compliance Checklist.

PREPARING FOR A DATA SECURITY BREACH
Companies should have a plan in place to respond to a data security breach before a breach occurs. In fact, several compliance regimes, such as HIPAA and the Payment Card Industry Data Security Standard (PCI DSS), require that businesses have incident response plans.

While the plan’s specifics vary depending on the business’s nature, the plan should include, at a minimum:

- A standing security breach response team. Individual members of the team may vary depending on the specific breach that arises, but the team should include representatives from:
  - legal;
  - the data or privacy office, or both;
  - corporate security;
  - information security;
  - human resources;
  - the business unit affected;
  - internal audit; and
  - public communication or media relations.

- A written incident response plan setting out procedures to follow in the event of a data security breach. The plan should specify each step to be taken once a breach is suspected and identify individuals responsible for each task. As part of the written plan, the business should also consider developing procedures for:
  - investigating the incident;
  - identifying affected individuals and obtaining their contact information;
  - providing notification to affected individuals where appropriate (see Developing a Notification Plan); and
  - creating a communications plan (see Developing a Communications Plan).

Businesses also may find it useful to develop model notice templates that can be tailored to the particulars of the incident if a breach occurs (see, for example, Standard Document, Data Security Breach Notice Letter (http://us.practicallaw.com/3-501-7348)).

As part of their preparation, businesses should also:

- Consider insurance coverage. Because of the high cost of responding to data breach incidents (see Box, Costs of a Data Breach), businesses should carefully review their existing policies and consider obtaining appropriate insurance coverage. Businesses should not rely solely on traditional legacy policies without carefully considering their risk profiles and determining whether cyber insurance coverage is appropriate and, if so, the scope of that coverage. For more information on insurance coverage, see Practice Note, Cyberinsurance: Insuring for Data Breach Risk (http://us.practicallaw.com/2-588-8785).

- Develop relationships with vendors. Responding to a data breach frequently involves the assistance of various experts and vendors, including outside counsel, forensic specialists, credit monitoring service providers, notification mailing vendors, public relations professionals and call center operators. Timing is crucial when responding to a data breach. Vetting and negotiating agreements with vendors in advance provides the opportunity to negotiate terms without the immediate pressure of responding to a breach and ensures that a business can move quickly when a breach occurs.

- Test the response plan. Ensure team members know their roles and test the plan to ensure the business is prepared to respond appropriately.
INVESTIGATING AND ANALYZING A BREACH

On discovering a possible data breach, the business must begin immediate mitigation and incident analysis. This consists of five primary steps, some or all of which may overlap and occur simultaneously:

- Convening the response team (see Convene the Response Team).
- Containing the data security breach (see Contain the Data Security Breach).
- Collecting data related to the breach (see Collect Data Related to the Breach).
- Analyzing the facts surrounding the breach (see Analyze the Facts Surrounding the Breach).
- Analyzing the contract and legal implications of the breach (see Analyze Contract and Legal Implications of the Breach).

Convene the Response Team

The business should already have a standing security breach response team in place as these incidents may require coordination by multiple individuals across many business areas (see Preparing for a Data Security Breach). Depending on the nature and scope of the incident, it may be advisable to:

- Set daily status calls to ensure that the team is accountable and moving forward quickly to investigate and respond to the breach.
- Take steps as appropriate to conduct incident investigation under attorney-client privilege by having the investigation performed at the direction of counsel and for purposes of providing legal advice. For example, institute communications protocols to provide that counsel be included on all communications.
- Institute other communications protocols, such as restricting communications to essential personnel, and if necessary, for example, where computer networks may be compromised by a breach, limit communications to only certain modes or designated channels.
- Prepare a media holding statement that can be revised as facts develop to ensure that the business is prepared to make an announcement quickly if required.

Contain the Data Security Breach

As soon as the business becomes aware of a data breach, it should take all necessary steps to investigate the incident and limit further data loss or intrusion. The business should also determine whether other systems are under a threat of immediate or future danger. For example, the business may need to:

- Immediately secure the physical area housing the data if the breach involves data stored physically on company premises.
- Isolate all affected systems and determine whether to take additional technical measures to contain the incident, such as changing passwords and administrative rights, in the event of a system intrusion.

Collect Data Related to the Breach

The business should immediately begin to collect available data related to the breach, including:

- Date, time, duration and location of breach.
- How the breach was discovered, who discovered the breach and any known details surrounding the breach, such as:
  - method of intrusion;
  - entry or exit points;
  - paths taken;
  - compromised systems;
  - whether data was deleted, modified or viewed; and
  - whether any physical assets are missing.
- Details about the compromised data, including:
  - a list of affected individuals and type (for example, employee, vendor or customer);
  - data fields (including all fields of personal information);
  - number of records affected; and
  - whether any of the data was encrypted and if so, what fields.

It is also important to preserve all data and evidence, including forensic evidence, collected in the event of any later legal or regulatory action. The business should also keep a log of actions taken during the investigation.

Analyze the Facts Surrounding the Breach

The business should collect and evaluate the facts to determine the incident's root cause and should identify:

- Whether personal information was compromised.
- The nature of that personal information, including specific data elements.
- The affected persons.
- The potential scope of the incident.
- The likely use of or access to the compromised data and, for purposes of some laws, the likelihood of harm to individuals.

The business should consider seeking the assistance of specialized consultants in capturing relevant information and performing computer forensic analysis. This especially applies if:

- The scope of the breach is large.
- It is difficult without this analysis to identify whether or not there was unauthorized access or acquisition of relevant data and in what manner, and who and what data or persons were affected.

Analyze Contract and Legal Implications of the Breach

In-house counsel should determine whether to contact outside legal counsel for assistance. Legal analysis should include analysis of:

- Relevant contracts and policies for notification and other obligations.
- Breach notification requirements.
- Insurance coverage.
- Indemnification obligations or rights.
- Litigation risk.
- Law enforcement investigations (see Box, Contacting Law Enforcement).
- Employee liability or employment action the business should take as a result of the breach.
DESIGNING A COMMUNICATIONS PLAN

Developing messaging may be difficult because of the ongoing development of facts or limitations law enforcement places on communications. However, developing a communications plan requires thoughtful consideration as it is important to be consistent, transparent and responsive while also considering reputational harm and legal risk. Communications should be accurate, while taking into account and providing for unknown information or the potential for the knowledge of facts to change.

The size of the incident generally drives the nature and scope of the communications plan. The plan should:

- Account for both internal and external communications.
- Address both traditional and social media.

Internal Communications

Because of possible legal action, haphazard internal communications can significantly burden the business in the event it must respond to requests for information from regulators or litigation discovery. Poorly devised employee communications can also bleed over into external communications given the ubiquity of email. The internal communications plan should address communications with:

- Employees. Communications with employees should be consistent and, with the exception of "need to know" personnel, contained and designed to provide information similar to that being provided to the public.
- Other stakeholders. The internal communications plan should provide for ongoing communications with the executive team, the board of directors and other stakeholders, such as business partners.

Communications with the Media

A business may handle media communications internally or by engaging a public relations (PR) professional, or both.

Even if the business has an internal media relations team or has an existing relationship with a PR firm, the business must carefully evaluate whether the team has experience with crisis management communications and whether it may be appropriate to engage a professional experienced in working with companies managing a data breach.

Communications with Affected Individuals

Once the business has determined notification is necessary, notice to individuals should occur expeditiously, consistent with legal obligations (see Developing a Notification Plan).

Beyond the specific legally obligated notice, businesses must be ready to further engage with affected individuals. Many state data breach statutes require notification letters to include contact information for someone to whom individuals can direct questions. Even if not required, as a matter of customer relations and risk management, this information should be provided along with a specific outlet for customer questions. Businesses should consider the following communications tools:

- Frequently Asked Questions (FAQs). The business should prepare FAQs and responses regardless of the chosen communication method. Persons responding to inquiries should be trained in how to use the FAQs. The business should review the FAQs continually throughout the notification process to ensure accuracy and responsiveness.
- A dedicated toll-free telephone number. Regardless of other modes of communication the business may employ, affected individuals will likely call with questions. It is often better to be prepared by providing a dedicated line for those calls. A business should consider whether it can handle calls internally or should engage a call center. This will depend on the size of the incident and the nature of the business. For instance, a business may decide to handle calls internally if it already has an existing call center.
- A dedicated email address where customers may send questions. For smaller incidents, or incidents that affect certain populations, businesses may find that setting up an email address, whether alone or in addition to a dedicated phone number, is appropriate. If so, these emails should be frequently monitored, given timely responses and the person(s) responding should be trained on the FAQs and messaging strategy.
- Posting information on the business’s website. In addition to direct modes of communication, businesses should consider posting information on their websites, including contact information for direct modes of communication.

Regardless of the mode of communication, businesses should document communications with affected individuals and have an escalation process in place so that they quickly and adequately respond to any inquiries that the FAQ answers cannot address.

DEVELOPING A NOTIFICATION PLAN

When legally required or desirable for other reasons, such as customer relations, the business should develop a notification plan for affected persons, or if the business is a service provider holding information for another business, those third-party businesses.

If the business provides notice, it should promptly decide on the channel of notification and the content of the notices and notify affected persons as soon as possible, all subject to applicable legal requirements. However, businesses should carefully assess whether it should notify individuals where not legally required due to legal and reputational risks associated with over-notification. (See Box, Risks of Over-notification.)

Identify Legal Obligations

As a foundation for preparing a notification plan, a business must identify its legal obligations. This requires identifying:

- The types of data compromised.
- The affected persons.
- The jurisdictions involved (typically, the place of residency of the affected persons).
- The state, federal or international laws triggered by the data and jurisdictions involved.
- Whether there are any notification obligations as to:
  - individuals;
Breach Notification

- third-party businesses (for example, if the business is a service provider);
- regulatory agencies;
- law enforcement; or
- consumer reporting agencies.

If the business is a public company, the materiality of the impact of a breach on the business to assess whether an SEC Form 8-K filing is warranted.

Notification

Once the business has identified its notification obligations, it can develop and implement a notification plan. The notification plan should address the following issues:

- Preparing a list of persons to be notified, including addresses. Preparing the list of individuals may be done by reference to the compromised data itself, to the business’s contact database or a combination of both. Preparing the notification list for a large incident frequently requires the participation of both external forensics consultants and the internal IT team.

- Determining the method of notification. The applicable laws determine the method of notification. In most cases, practical considerations effectively require notification to affected persons by mail. If so, the business should analyze whether it can handle the mailing internally or if it should engage a mailing notification vendor. When working with a mailing vendor, the business typically provides the template letters and the notification list to the vendor. The vendor then may run the addresses against the national change of address database, generate the letters and mail the letters to individuals. The vendor may also provide services related to return of service and undeliverable mail.

- Drafting the notification. The applicable laws determine the contents of the notification. In many cases, it is impossible to draft just one notification that can be sent to all affected individuals because of jurisdiction-specific content requirements. A common approach to dealing with this issue is to draft one form of letter that satisfies the requirements of most affected jurisdictions and then state-specific letters to be sent to individuals in those states where the universal letter is not appropriate. Different forms of letters likely will have to be drafted for notice to representatives of affected minors and deceased persons if warranted, particularly if the business offers remediation services.

- Drafting the substitute notice or notice to the media, if any. In many cases, the business may choose to or may have to provide substitute notice because of:
  - the costs of notifying;
  - the number of people affected; or
  - the lack of good contact information for affected individuals.

Providing substitute notice may require notice to the media or publication in media depending on the jurisdiction and number of individuals affected.

- Remediation services. Offering appropriate remediation services can have an impact on consumer goodwill and can affect litigation outcomes. The notification plan also should address whether to offer affected individuals any or a combination of the following:
  - credit monitoring services;
  - identity theft insurance;
  - the cost of credit freeze services;
  - identity theft help information packets; or
  - compensation for identity theft.

(See Box, Determining Whether to Offer Remediation Services.)

POST-NOTIFICATION

Even after containing and analyzing a data breach and notifying affected individuals, businesses should not consider the matter closed. Significant legal action may follow, but even if it does not, the business should study the incident to assess the adequacy of its response and to determine if it should make changes to its data breach response or data security programs.

After experiencing a data breach, a business should:

- Prepare for litigation and regulatory action. The business should consider litigation matters that may arise, including:
  - civil lawsuits, including putative class actions, instituted by individuals whose personal information was compromised, including shareholders or other businesses whose data may have been impacted by the breach;
  - an investigation of the business or specific employees, its customers or its service providers by law enforcement authorities and state or federal regulatory agencies;
  - Congressional inquiries and requests to testify; and
  - indemnification claims it may have against third parties if third parties are at fault for a breach.

- Consider whether an SEC filing is warranted. Public companies must assess whether a particular data breach rises to the level of a material incident in terms of the impact on investors’ investment decisions. In those circumstances, the incident may, apart from the individual notice process, warrant a public Form 8-K filing with the Securities and Exchange Commission.

- Review information technology systems and physical security. The business should conduct follow-up analysis of the breach to determine root causes. It should review applicable access controls and procedures (both those in place before the breach and those put in place as the result of containment efforts) to ensure that it has addressed and resolved weaknesses.

- Assess operational controls. It is important to:
  - assess business operations to determine necessary revisions to data collection, retention, storage and processing policies and procedures;
  - assess the need for additional employee training in data protection policies and processes; and
- review agreements and policies to determine whether they need any updates or modifications. This includes agreements with third parties that handle personal information, website privacy notices and terms of service, agreements with customers or other third parties and employee handbooks and policies.

- Evaluate the response. After the business responds to the breach, it should evaluate its response and implement changes or additional measures to eliminate vulnerabilities and improve effectiveness in preventing and responding to future breaches.

### COSTS OF A DATA BREACH

According to a recent benchmark study of data breaches of 100,000 or less customer records:

- The average cost of a data breach in the US in 2013 was approximately $201 per customer record.
- The total cost of a data breach in 2013 ranged from about $135,000 to $23 million, with the average cost being $5.8 million.

These costs include:

- Costs spent to detect and contain the breach, notify affected individuals and implement post-breach responses.
- Lost business due to reputational damage.

(Ponemon Institute, LLC, 2014 Annual Study: Cost of a Data Breach.)

Additional costs may include:

- Drops in share price for public companies.
- Payment of government fines and penalties, including those imposed by the FTC for violating a consent decree or if the business is subject to certain regulations, a specific rule and state attorneys general, for failing to provide proper notice to consumers or for not reasonably protecting personal information.
- Defending against lawsuits brought by private plaintiffs, including affected individuals, shareholders or other businesses.

### CONTACTING LAW ENFORCEMENT

Consult legal advisors before notifying law enforcement of a breach to determine whether notice is advisable and the appropriate response to any law enforcement inquiry. If necessary:

- Contact appropriate local or federal law enforcement to enable immediate deployment of investigative capabilities.
- Assign one member of the security breach response team the responsibility for interfacing with law enforcement agencies.

Law enforcement authorities may request a delay in notification of affected persons or release of public information if they would hamper law enforcement investigations. Local or federal law enforcement authorities also may desire to conduct an investigation into the business’s security systems and its response to the breach as a part of their investigation of the incident.

Even if not required by law, consider whether:

- To file a police report for the incident (for example, for a stolen laptop or burglary on the premises).
- It makes sense to contact state attorneys general or regulators even if not legally required.

### RISKS OF OVER-NOTIFICATION

Over-notification refers to situations where:

- A statutory trigger, for example, unauthorized acquisition, prompts notification even where the personal information is not at risk (for example, information that is misdirected to a reputable and trusted vendor that certifies it destroyed the information).
- A business notifies persons, though it may not be legally required to do so, to avoid potential liability in the event the facts or circumstances of the breach may later be interpreted by regulators or others to have required notification under one or more of myriad laws that may apply.
- It is difficult to ascertain the precise identity of the persons or nature of information affected by a potential breach incident, prompting a notification of all possibly affected persons even though their information may actually be unaffected.

Over-notification negatively affects both consumers and businesses. Costs to businesses, which may ultimately be passed on to consumers, include unnecessary:

- Legal fees.
- Costs for preparing and delivering notices.
- Litigation and regulatory defense costs.
- Reputational harm.

In addition to numbing consumers to real threats to their information, over-notification also contributes to an increase in the data breach noise that may cause a heightened ability of fraudsters to capitalize on individuals’ fears. Recognizing this risk, following well-publicized breaches, the FTC and state consumer protection agencies frequently have warned consumers about phishing and other scams designed to prey on those fearful of having been the subject of a breach.
DETERMINING WHETHER TO OFFER REMEDIATION SERVICES

There are various commercial remediation services available, including:

- Credit monitoring.
- Products offering assistance to persons experiencing fraud on their accounts.
- Identity theft insurance.

For years, businesses have customarily offered at least one year of free credit monitoring to affected persons. This is especially the case where the data breach implicates information that others can use to carry out identity theft, such as Social Security numbers or driver’s license numbers because of the increased risk of fraud associated with loss of that information.

Traditional credit monitoring typically includes notification to the covered person of:

- Changes to the person’s credit file maintained by one of the major consumer reporting agencies.
- New credit inquiries.
- New accounts opened.
- Reports of delinquent accounts.

Offering credit monitoring following a breach helps companies demonstrate they are taking measures to help protect affected individuals. However, credit monitoring is not particularly helpful in detecting existing financial account fraud, such as unauthorized credit card charges, since a name and stolen card number are generally not sufficient to allow a criminal to open a new credit account, but that information can be used to make fraudulent charges.

In recognition of this, several attorneys general, such as those from California and Illinois, have released guidance pointing out that credit monitoring is not helpful for account number breach. Guidance from California, for example, recommends that if a business offers credit monitoring or other assistance it should “make sure it is relevant to the situation.”

While credit monitoring services may not be germane, businesses experiencing breaches of their customers’ account information have increasingly offered credit monitoring. In some cases this has occurred because regulators have pressured businesses to offer it regardless of its relevance. In other cases, it is because of a desire by the company to provide something to consumers, even though the service may not address the particular incident, perhaps hoping to stave off litigation.

New amendments to California’s data breach statute, effective January 1, 2015, may actually require that businesses offer free credit monitoring to California residents for 12 months if the notifying entity was the source of the breach and the breached information included affected persons’ names, plus:

- Social Security numbers.
- Driver’s license or California identification card numbers.

Some commentators have suggested that the new amendments do not require offers of credit monitoring and instead interpret the amendments to require businesses that choose to offer credit monitoring to do so for a period of at least 12 months and at no charge. Because of ambiguity in the statutory text, however, the law could be interpreted as mandating credit monitoring for at least 12 months. Following the more strict interpretation should not significantly affect the credit monitoring offer practices of many large companies, but it may have a more significant impact on smaller companies.

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at practicallaw.com. For more information or to schedule training, call 888.529.6397 or e-mail training.practicallaw@thomsonreuters.com.