# A data breach can happen anytime. Be ready to respond.

LifeLock BREACH SOLUTIONS

**BEST PRACTICES**

It only takes one stolen laptop, one employee's USB stick, one hacker, one virus, or one careless error to compromise your company's reputation and revenue. The threat of data breach is real and it's critical that your company is prepared. A thorough plan that can be executed quickly is essential to comply with relevant regulations, maintain customer loyalty, protect your brand and get back to business as soon as possible.

## QUESTIONS TO ADDRESS WHEN A BREACH OCCURS

### WHAT IS THE TOTAL SIZE OF THE BREACH?

This may seem like an easy question to answer but in reality, determining the total size of the affected population can be difficult. It is important to establish the forensics capabilities necessary to rapidly determine the size of the breach BEFORE a breach occurs.

### WHAT TYPE OF DATA LOSS OCCURRED? WAS IT ACCIDENTAL DATA LOSS OR CRIMINAL INCURSION?

Understanding the reason for the breach will help understand your risk, and the corresponding risk to the affected population with respect to likelihood of near-term criminal use of the compromised identities, and knowing that can help you determine your communications, as well as breach response product selection/capabilities.

### WHAT ARE OUR LEGAL AND REGULATORY OBLIGATIONS? WHO MUST BE NOTIFIED?

47 states have laws stipulating who must be notified in breach situations.[1] Do any industry regulations, internal policies, contracts or voluntary association rules apply? Financial institutions must notify consumers and regulators.[2] Healthcare providers must provide public and industry notification of any data breach.[3] Breached merchants must comply with all applicable state, federal and industry security and notification requirements. It is important to identify and maintain a repository for tracking those regulations for every state in which you have an employee or customer presence.

**Identity theft**
tops list of consumer complaints for 14th consecutive year.[4]

**2,164**
The number of breach incidents reported in 2013, exposing 822 million records.[5]

**1,000,000**
The number of records exposed by just twenty-seven breach incidents in 2013.[6]

**63%**
Percentage of consumers who believe that organizations should be obligated to provide identity theft protection.[7]

**+**
43% of consumers say a sincere and personal apology would encourage them to continue a relationship with a breached company, while 41% would prefer free ITPS.[8]

[1] ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[2] ithandbook.ffiec.gov/media/resources/3372/frb-sr-05-23.pdf
[3] hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[4] FTC Email Scam Alerts (2014) "Identity theft tops list of consumer complaints for 14th consecutive year"
[5] 2013 Data Breach Trends, Risk Based Security Report (Feb 2014)
[6] Ibid.
[7] Ponemon Institute, "The Aftermath of a Mega Data Breach" report, 2014
[8] Ibid.

## QUESTIONS TO ADDRESS WHEN A BREACH OCCURS

### WHAT LEGAL AND PUBLICITY EXPOSURE DO YOU ANTICIPATE AS A RESULT OF THE DATA BREACH?

Consider the cost of breach response and the cost of lost business. A data breach can put your financial stability at risk by increasing costs and decreasing revenue. Studies have shown that one of the biggest losses from data breaches result from lost consumer confidence and resulting lost business.[9] That's why it's important for businesses to anticipate the level of media exposure and consumer or employee blowback when deciding how to respond to a breach, and which service(s) to make available to the affected population.

### WHAT IS THE SCOPE OF THE BREACH? WHAT TYPES OF INFORMATION WERE COMPROMISED?

Social security numbers? Addresses? Credit card information? Bank account information? Knowing the type and extent of the lost data can guide your selection of a breach service offering and your communication plans. If the data loss included credit card numbers, for example, but did not include Social Security numbers, then the service should include credit card transaction monitoring capabilities and should not necessarily need to include the ability to identify new applications for new lines of credit. Correspondingly, if Social Security numbers were compromised, the breach response product should include new application alert capabilities.

### WHAT IS YOUR COMMUNICATIONS STRATEGY?

Understanding your communications strategy begins with understanding the SIZE, TYPE, REGULATORY requirements, EXPOSURE implications, and SCOPE of the breach in question. A firm understanding of those elements of the breach can position you to answer the 'how,' 'what,' 'when,' and 'where' questions related to breach response. For example, the number and types of communications you will employ, when you will employ them, and what product you will offer to the affected population for protection, as well as the duration of the subsidized protection.

The law dictates what you must do, but your employees and customers expect more. Meeting only minimal legal requirements could mean maximum damage to your brand.

### HOW YOU HANDLE A BREACH SAYS A LOT ABOUT YOU.

To facilitate a fast response, your institution should have developed an incident response playbook and appointed a leader to be in charge of it. The team to carry out the plan should be cross-functional with heavy emphasis on communications and public relations, since reaching out to the affected population will be the most important aspect. Other departments that make up an effective team include: analytics to determine the impacted population; the fraud group to put a timely stop to the violation; legal to notify regulators; customer service to handle inquiries and claims; and an identity theft protection unit to provide identity theft protection solutions where applicable.

Regaining trust is hard to do after a breach. Don't make it more difficult by offering only limited protection for your customers. With LifeLock Breach Solutions, you can offer comprehensive identity theft protection available to help protect against criminals who can sell their credit and wreak havoc on their lives. When you provide more than just limited protection, like credit monitoring alone, you'll increase the potential to regain trust.

Pre-define your organizational roles and responsibilities, understand legal regulations and requirements, and negotiate breach response relationships BEFORE a breach occurs so that you can be ready to respond with identity theft protection services that protect your valuable brand and customers.

## How to act in a crisis if a breach occurs:

1. Fulfill Federal & State notification requirements.
2. Calm victims and investors.
3. Have a proactive plan in place: if identities are compromised, help protect against further damage.

[9] reuters.com/article/2014/04/04/us-target-lawsuites-idUSBREA3309J20140404

## QUESTIONS TO ADDRESS WHEN A BREACH OCCURS

### BREACH RESPONSE NEGOTIATION CONSIDERATIONS CAPABILITIES

What are the product capabilities of your preferred response provider and do those products support monitoring and alerting the data you may be at risk of losing? For example, if you maintain payroll data (account and routing information) does the preferred response provider offer services capable of monitoring bank accounts and alerting on potential account takeover incidents? Can the provider monitor the identities of individuals younger than 18? How many alerts does the company issue on a monthly basis?

**PRICING AND PRICING MODELS:** What is the 'cost per activated member' (your cost for each enrollment ) for the service(s)? Can the response provider support a "Population" pricing model wherein the entire affected population has access to enroll in the identity theft protection service at a net cost per member that is less than "cost per activated member" model?

**COMMUNICATIONS:** Can the response provider work with your team to create a communication template for immediate use in the event of a breach?

**ENROLLMENT PROCESS:** What enrollment vehicles can the response provider make available (online, phone, or both)? If phone enrollments are available, where is the provider's call center(s) located and during what hours can individuals call to enroll? What are the average phone hold times? If enrollment is available online, what does the enrollment experience look like, is it the website "professional" and does it clearly describe the product features being offered?

**POST-ENROLLMENT MEMBER EXPERIENCE:** Which metrics does the preferred response provider use to measure member satisfaction? What is the provider's annual member retention rate for PAYING members? Does the provider use well established member/customer satisfaction indexes to monitor its performance (e.g., the Net Promoter Score)?

**ALERTING FREQUENCY AND IMMEDIACY:** How many and what types of alerts are issued to the members of the breach response product; and how soon after an new application is opened does the response provider issue the alerts?

**REPORTING:** What kinds of reports will the response provider make available to your company with respect to member enrollment totals and information on the frequency and types of alerts issued to the affected population? To what frequency of reporting will the provider commit?

## INTERNAL THREATS TO CUSTOMER DATA SECURITY

- Employee negligence and faulty business processes
- Confidential information sent to or from a home account
- Email inadvertently sent to the wrong person
- Customer data sent over a public WiFi network
- Customer data loaded to a mobile storage device (portable hard drive, flash drive, CD, DVD, etc.)
- Malicious employees
- Email with intellectual property sent to a competitor
- Unauthorized employee accesses an unsecured computer or server
- Customer data accessed by system administrator or IT personnel
- Packet sniffing application used to scan internal network traffic for key words
- Ineffective methodologies for keeping track of what customer information is collected and where it is stored
- Malicious IT staff member at business gains access to confidential files or records provided by your company to senior management

## EXTERNAL THREATS TO CUSTOMER DATA SECURITY

- Ex-employee access to network traffic using an account that has not been disabled
- Competitor monitors external traffic to scan for key words
- Hacker monitors public WiFi connection or an intermediary mail relay server
- Thief steals a laptop at an airport
- Traveling employee loses track of portable media in transit (e.g., leaving a flash drive connected to a customer or partner's computer)