CSR®

Data Life Cycle Management

CSR Breach Reporting Service™
Frequently Asked Questions

Quick and Complete Reporting is Critical after Data Loss

About the CSR Breach Reporting Service™:

Requirements to Protect Data and Breach Reporting

Billing Questions

About CSR

Confidential and Proprietary
© 2015 CSR. All rights reserved. CSR refers to the corporation CSR Professional Services, Inc.

Quick and Complete Reporting is Critical After Data Loss

Why do businesses need this service?

All organizations that have employees, customers or vendors must, by law, comply with requirements to report and notify consumers of the loss, or suspected loss, of personally identifiable information.

If organizations don't have this service, what could happen?

Failure to report actual or suspected data loss – whether accidental or criminal, within legally mandated time frames may lead to fines, as well as civil and criminal sanctions.

For example, the Visa can assess fines of up to $100,000 per breach against businesses that fail to properly report an incident.

Lost trust means lost sales. The fallout of data breaches has caused businesses to close their doors. The FTC and Visa recommends that businesses plan ahead to reduce risk.

Why companies shouldn't try to do this themselves

Liability rests entirely with you, as well as civil and criminal sanctions, on both state and federal levels. Penalties for missing just one report to authorities can be $15,000-100,000.

New rules continue to take effect, types of data that must be protected increase, and additional agencies pile on new requirements. Short time frames to meet requirements make the learning curve unrealistic.

Trained, certified privacy professionals use a proprietary system to evaluate your circumstances against hundreds of rules and regulations to determine whether reports need to be filed and/or consumers, consumer credit bureaus, and other entities notified.

About the CSR Breach Reporting Service™

What is the CSR Breach Reporting Service™?

CSR's team of in-house privacy professionals use a patented, award-winning service to fulfill your mandated requirement to comply with federal, state and other laws to report the loss of personally identifiable information to authorities and notify affected individuals.

How does this service work?

It's a simple process. In the event that personally identifiable information is lost, or suspected to be lost, stolen or compromised:

1) You call the toll-free number
2) Privacy expert interviews you
3) Privacy review panel determines
    a. If reports need to be filed with authorities
    b. If notification needs to go to consumers and/or others
4) Reports are filed with authorities

Confidential and Proprietary
© 2015 CSR. All rights reserved. CSR refers to the corporation CSR Professional Services, Inc.

5) You are notified of reporting and whether consumer notification is required

6) You provide input for privacy expert to implement consumer notification

What number do I call in the event I think I have lost personally identifiable information?

In the event you believe you may have lost personal data, call the toll free number provided in your welcome packet or call customer service at Richards & Richards to retrieve it.

What are the hours of your service?

The operators are available 24/7 every day of the year for you to call.

How do I sign-up?

You are automatically enrolled. To learn more about data protection and breach reporting, go to http://richardsandrichards.com/csr-breach-reporting/.

Is this breach insurance?

No. This is not breach insurance. The Breach Reporting Service™ is not an insurance product. It is a service to provide breach reporting and consumer notification. Insurance provides payment for loss.

Will you notify my customers or provide other post-breach services?

Yes. Privacy experts will work with you to notify customers. You can also engage the privacy team for additional services separately. Contact us for further information.

Will this service share the details of my reports?

The privacy professionals are not allowed, by law, to relate details to anyone other than the authorities who mandate reporting.

What if I'm not sure whether I have lost data?

You should still call the toll free number provided in your welcome packet or call customer service at Richards & Richards to retrieve it. Leave it to the privacy professionals to determine whether any reports need to be filed or consumers notified.

Requirements to Protect Data and Breach Reporting

What is personally identifiable information?

The simple answer is it's anything that can be used to identify you. The loss of this information leads to identity theft.

Types of personal information include: name, address, phone, email, birthdates, Social Security numbers, driver's license, bank account and credit card information and the list continues to grow with new and revised legislation and court rulings.

Other personal information includes health information, medical records, Vehicle Identification Numbers, license plate numbers, login credentials and passwords, school records as well as voice recognition files. Fingerprints, retina scans, and handprints are also considered personal information.

What is the difference between PCI and personal information?

Confidential and Proprietary
© 2015 CSR. All rights reserved. CSR refers to the corporation CSR Professional Services, Inc.

PCI data is just one type of personally identifiable information. The PCI Data Security Standard protects credit cardholder data such as debit or credit card number, expiration date and card security code.

What is a breach of personally identifiable information?

The unauthorized access, loss, use or disclosure of information by either accident or criminal intent which can identify an individual.

What is data breach reporting?

When a breach occurs the clock starts ticking to comply with federal, state and other laws. Reporting involves the where, when and how of the incident.

What is consumer notification?

Almost every state has enacted a data breach notification statute. These laws generally require businesses that have personal information about residents within a state notify those residents when that data is compromised.

What are some examples of a breach?

A breach can occur in many ways, including through lost laptops or smart phones, improper disposal of paper records, or intrusion into your network or PC by hackers. The definition continues to expand.

Who do you need to report a breach to?

Over 100 countries, as well as 300 federal, state and local authorities in the U.S. and Canada require reporting. Reports may also need to be filed to Visa, MasterCard and other non-governmental entities.

What laws govern personally identifiable information?

Here are a few examples of the hundreds of laws and regulations that relate to the protection of personally identifiable information and requirements to report suspected or real loss.

- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Drivers Privacy Protection Act (DPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic Clinical Health (HITECH) Act
- Payment Card Industry Data Security Standard (PCI-DSS)
- Family Educational Rights and Privacy Act (FERPA)
- 47 state data breach laws

Who are the enforcement agencies and others who might be involved after a breach?

Enforcement officials include various federal and state agencies as well as attorneys general, commissioners and others. Here are a few examples:

- Federal Bureau of Investigation (FBI)
- US Secret Service
- Federal Trade Commission (FTC)
- Dept. of Health and Human Services/Office of Civil Rights

Confidential and Proprietary
© 2015 CSR. All rights reserved. CSR refers to the corporation CSR Professional Services, Inc.

- Card brands like Visa, MasterCard, etc.
- State Attorneys General

What if personally Identifiable information shared and/or received from another organization is compromised?

If your business is a third-party provider and has personally identifiable information on customers, employees, or vendors, then you may be required to notify authorities and/or consumers and others that a breach, or suspected breach, has occurred.

What if personally Identifiable information under my care is encrypted, redacted, or masked?

Even if the material is encrypted, redacted, or masked, various regulations still require you to report. If it is encrypted, and the encryption key has been potentially compromised, reporting is required and/or notification is required.

Billing Questions

How much does this cost?

Just $14.95/month gives you 24/7 access to the Breach Reporting Hotline. Privacy professionals will collect information used to determine whether breach reports need to be filed and to whom, and whether consumer notification is required. This relieves you of the legally mandated, time-sensitive tasks. There is no additional cost to file reports with authorities. Most often, consumer notification is done by email. In the rare case that surface mail is required, there will be a nominal fee.

A business seeking services from a consultant, an accountant or attorney would pay tens of thousands of dollars.

Can I opt out of the program if I don't want it?

Yes, however we don't recommend it. We provide this service at an affordable price to enable you to comply with mandated reporting in the event of an incident. You'll have privacy experts who will relieve you of this burden. If you opt out, you will be responsible for all liability as well as civil and criminal sanctions.

Can I opt out later after I see how it goes?

You can opt out at any time, but remember you will be responsible for all liability as well as civil and criminal sanctions.

I received a letter about a data breach reporting program. Why did you put me in this program?

We strongly believe that it's our duty to protect our customers as much as possible from events that can harm their business.

To meet mandatory requirements related to suspected or actual loss of personally identifiable information of employees, customers and vendors, we provide an affordable breach reporting solution.

If you have an incident, CSR's service will file required reports and complete consumer notification with your input.

Confidential and Proprietary
© 2015 CSR. All rights reserved. CSR refers to the corporation CSR Professional Services, Inc.

About CSR

Who is CSR?

CSR Professional Services, Inc. is a leading provider of award-winning data life cycle management and expert services for businesses domestically and around the globe.

CSR enables compliance with Personally Identifiable Information (PII) requirements while facilitating best practices to reduce the business risk and financial liability associated with the acquisition, handling, storage, sharing and disposal of data.

How many companies use this service?

Hundreds of thousands of businesses have enrolled in this breach reporting service.

What qualifications do these "experts" have to collect this information and file reports?

These experts have all received and maintain one or more certifications from the International Association of Privacy Professionals. Specialties vary from U.S., Canada, Europe, to IT, Government and the CIPM designation for Certified Information Privacy Manager.

Can you help me with other privacy services?

Other services include personally identifiable information business analysis, remediation, audit, forensic, education, certification, special projects and Stand-In Privacy Officer provision. For further information, email sales@richardsandrichards.com.

Confidential and Proprietary
© 2015 CSR. All rights reserved. CSR refers to the corporation CSR Professional Services, Inc.