CYBERSCOUT™
WE'LL TAKE IT FROM HERE™

ASSURANCES PALLADIUM INSURANCE

Information Security Breach Response Plan

A Step by Step Guide to Instituting
CyberScout Breach Services

Table of Contents

Procedures for Initializing Security Breach Response Services

Introduction

The following document is to be used by your Company in case of an Information Security Breach exposing the personally identifiable information (PII), Protected Health Information (PHI) and/or Non-Public Personal Information (NPPI) of your Customers, Clients, Patients, Employees, Staff or other Data Subjects. This document should be stored with your Business Continuity Plan and should be an integral part of your internal Information Security Breach Response plan. This document provides relevant contacts and thorough procedures to follow once it has been ascertained that your Company has suffered an Information Security Breach exposing PII. (hereinafter referred to as a "Breach" for purposes of this document.) Any and all processes in this document can, and in many cases should be supplemented by additional support processes as may be needed based on regulatory and other requirements and needs.

In order to expedite the proper internal communication and handling of each and every Breach incident, having the most up to date information is essential. Therefore, please be sure to complete and fill in all required information in this plan. Further, you should update your Company's procedures and contacts on a quarterly basis to make sure that all contacts and information are accurate and current.

The following document is not a legal document nor should it be misconstrued as the giving of legal advice. This document is meant merely to facilitate the proper implementation of CyberScout Breach services for your Company under an agreement with you insurance provider or directly with CyberScout.

However, all information/communication regarding a Breach, or suspected Breach, is considered confidential information and **will not** be disclosed by CyberScout to any third parties unless authorized to do so or compelled by law enforcement or court order.

Primary Company Contacts in Case of a Breach

The following pages contain contact sheets for your Company to utilize internally should an actual Breach occur. The information should better help your staff in dealing with the appropriate authorities as well as with CyberScout staff. The information is to be used by your Company only and does not need to be provided to CyberScout. When and if an incident occurs, we will simply require a completed Appendix A, which contains pertinent contact information.

Please be sure to update the contacts to reflect new staff or changes in leadership at least annually.

The information provided for these contacts will likely be the same contacts included in Appendix A. These are the primary contacts that CyberScout will communicate and work with when and if an incident occurs. However, during a Breach it is best to utilize one of these contacts as the "point" person to direct communications through.

Main Breach Supervisor and Outside Liaison

Responsibility: To oversee the handling of any and all Breaches occurring at the Company. This individual will be the main liaison and contact with CyberScout staff and will act as the main contact for law enforcement, regulators, and internal staff regarding a Breach. This is also the individual to whom all activity reports will be sent. This position is usually filled by the Company's Owner, CEO, CIO, CSO, CPO, President, or other high level staff (or appointed designee) with the ability to make high level decisions and communications.

Name: _____

Address: _____

_____

_____

Office Phone: _____

Home Phone: _____

Cell Phone: _____

E-Mail Address: _____

Emergency Contact: _____
(*Spouse, Family Member, etc.*)

Emergency Phone #1: _____

Emergency Phone #2: _____

Breach Response Contacts

Public Relations and Communications Liaison

Responsibility: To oversee the handling of any and all PR responses regarding a Breach, including preparing of or proofing of press releases and media responses as well as preparing Breach FAQ's for provision to CyberScout services.

Name: _____

Address: _____

_____

_____

Office Phone: _____

Home Phone: _____

Cell Phone: _____

E-Mail Address: _____

Emergency Contact: _____
(*Spouse, Family Member, etc.***)**

Emergency Phone #1: _____

Emergency Phone #2: _____

Legal and/or Compliance Liaison

Responsibility: To oversee requisite compliance steps and monitor and determine any legal implications of the Breach for the institution. Occasionally will provide oversight and review of the Breach notification letter to be sent to affected members of the Breach.

Name: _____

Address: _____

_____

_____

Office Phone: _____

Home Phone: _____

Cell Phone: _____

E-Mail Address: _____

Emergency Contact: _____
(*Spouse, Family Member, etc.***)**

Emergency Phone #1: _____

Emergency Phone #2: _____

Escalation/Customer Service Contact

Responsibility: To oversee and deal with member service and to act as an escalation contact should CyberScout need to refer a problematic or difficult Breach victim back to your Company. Please note that this individual may be the same contact as the Main Breach Supervisor and Outside Liaison contact, or may be a separate designated staff member.

Name: _____

Address: _____

_____

_____

Office Phone: _____

Home Phone: _____

Cell Phone: _____

E-Mail Address: _____

Emergency Contact: _____
(*Spouse, Family Member, etc.***)**

Emergency Phone #1: _____

Emergency Phone #2: _____

CyberScout Breach Contacts

Below you will find the Primary and Secondary Contacts at CyberScout to be notified in the event of a suspected or an actual Breach involving the personally identifiable information of your customers. Said contacts should be contacted immediately following the Breach of PII:

Insurer
You should provide you insurer claims contact information, policy number and instructions to Call your Insurer's claim departments to let them know of the incident and open a claim. They will facilitate contact with CyberScout.

CyberScout Breach Response team

Email: breach@CyberScout.ca
Phone: 866-989-3173

Relevant Primary Law Enforcement/Regulatory Contact Information

The following contact sheet is for use by your Company to keep track of the investigators handling your particular case. It is to be used by your Company for quick reference and auditing purposes. This document does not have to be provided to CyberScout.

Police

Name of Police Agency: _____

Lead Officer Name: _____

Office Tel: _____

Cell Phone: _____

E-Mail: _____

Canada Post

Lead Agent Name: _____

Office Tel: _____

Cell Phone: _____

E-Mail: _____

Summary and Quick Reference Guide

SBR Service implementation plan following a Breach involving Personally Identifiable Information of your Customers

1. Your Company should have an Information Security Breach Response Plan in place and should be revised to include the SBR Services described here. *(Page 10)*
2. Immediately following the discovery of a Breach, follow internal procedures for initiating the Information Security Breach Response Plan. *(Page 8)*
3. Contact your insurer in order to process a breach claim. Your claims representative will call CyberScout's breach response team.
4. As soon as CyberScout becomes aware of your situation, a member of the breach team will reach out to you to collect additional information. If you have a complete copy of the CyberScout Breach Services Client Company Incident Details Sheet found in Exhibit A, you can provide it to your CyberScout contact. *(Page 11 and Page 15)*
5. Upon assessing the situation, CyberScout will provide the Company with notification letter templates and an FAQ template that are customized to your needs. *(Page 12)*
6. Your Company should review and edit the notification letter and FAQs and determine if they wish to make additional proactive credit products available and if the notice mailing should be staggered. CyberScout should then be informed of the decisions. *(Page 10)*
7. The Notification Letter and FAQs should then be submitted to CyberScout for final review of the accuracy of the description of CyberScout services. *(Page 13)*
8. Upon final review of the Breach notification letter and FAQs, CyberScout will provide the Company with the requisite number of unique "generic" USER Codes for insertion into the notification letter. *(Page 13)*
9. Upon receipt of a final signoff by relevant law enforcement, regulators and/or management, your Company then mails the notification letters. *(Page 12)*
10. Your Company may opt to have CyberScout help in additional media notification if necessary and at no additional charge. *(Page 14)*
11. CyberScout begins handling affected customers' calls. *(Page 12)*
12. CyberScout provides periodic reporting to your Company regarding call volume. *(Page 14)*

Full Service and Procedural Description

SBR Service implementation plan following a Breach involving Personally Identifiable Information of your Customers

1. First and foremost, your organization should develop and implement an Information Security Breach Response Plan if it has not already done so. If an Information Security Breach Response Plan is not in place, your organization should create and implement one including the services covered under the SBR911 Services. If a plan is already in place, SBR911 Services should be integrated into your organization's Information Security Breach Response Plan. Your plan should be reviewed on a quarterly basis and should be revised annually at the least. It should be based upon input from your Company's leadership in the areas of legal, compliance, information technology, fraud and any other relevant departments.
2. Immediately following the discovery of a Breach, follow internal procedures for initiating the Information Security Breach Response Plan which should include initiating immediate notification procedures for involving:
    a. Corporate leadership (CEO, CPO, CSO, President, General Counsel, etc.)
    b. Law enforcement, if the loss may be the result of criminal activity such as the theft of a laptop, hackers, theft of information by an employee, or theft of equipment by employees or vendors. Relevant law enforcement may depend upon your particular situation and jurisdiction and may include:
        i. Local Police
        ii. Provincial Agencies
        iii. Canada Post / Postal Inspector
        iv. The Royal Canadian Mounted Police
    c. CyberScout Primary Contacts.
3. Contact CyberScout's Breach response team via E-mail and telephone:

    Email: breach@CyberScout.ca
    Phone: 866-989-3173

You must be able to provide the following information by filling out the *CyberScout Breach Services Client Company Incident Details Sheet* found in Exhibit A of this document and be able to submit this information in writing via E-mail. (If you unable to send electronically via E-mail then you may send via FAX). This information is required in order to best handle any Information Security Breach that discloses the PII of your customers. It is important to note that although you may not have all of the information available to you, the more notice you can give to CyberScout the better CyberScout can prepare for increased call volume and services. This information includes:

a. Company name
b. Incident Reference name
c. Primary contact name and information
d. Escalation contact name and information
e. Basic customer profile (i.e. checking account holders, patients, former customers, etc.)
f. Number of affected individuals
g. Discovery date of Breach
h. Approximate date that Breach occurred
i. Method of Breach
j. States of domicile/residence of affected data subjects (if known)

k. The type of information that was disclosed
l. Target date for notification letter mailing
m. Any additional credit products you wish to make available to victims on a proactive basis (at an additional charge to your Company.)
n. Billing contact for any additional credit products (if Company opts to offer such products proactively)

4. Upon receipt of a completed *CyberScout Breach Services Client Company Incident Details Sheet* found in Exhibit A, CyberScout will provide the Company with several notification letter templates and an FAQ template to begin the process of drafting the appropriate notification letter for affected data subjects. Some things to note when drafting your notification letter announcing the Breach and the resolution services/support:

   a. Your Company MUST receive clearance regarding any content describing CyberScout or any services provided by CyberScout.
   b. Any and all other content in the notification letter is the final responsibility of your Company. CyberScout will provide its own advice and consulting on wording of such notification letter however, any legal or regulatory liability for the content of such letter is the sole responsibility of your Company, and any such finalized letter should first be signed off on by your legal counsel and regulatory authority and/or law enforcement.
   c. If your Company wishes to begin the process of drafting FAQ's and the notification letter, sample FAQ language may be found in Exhibit B and sample notification letter content may be found in Exhibit C.

5. Depending upon the size and method of the Breach as well as the type of information and client base affected, the following additional services and procedures may want to be considered by the Company:

   a. Should the Company make additional PROACTIVE credit products available? *Products such as the ones listed below are available to the Company through CyberScout (or at your Company's election, your Company may contract with a third party provider of your choice to offer such additional services):*

      i. *Credit Reports*
      ii. *Both Bureau Monitoring*
      iii. *Single Bureau Monitoring*
      iv. *Additional Monitoring Products*

   a. ***If the Breach affects in excess of 100,000 data subjects***
   CyberScout can provide a special, dedicated informational website regarding the Breach, resolution services and possible proactive credit products. Should your Company opt to make additional credit products available through CyberScout then Breach victims could obtain these products through a secure password protected website. This option for making additional credit products available to victims via the information website following a Breach is only available for credit products purchased through CyberScout and not if your Company purchases such products through a third party provider.

   b. Should the mailing of letters be "staggered"?
   This practice is ALWAYS recommended in cases of large Breaches to avoid overwhelming your Company staff and CyberScout staff and to be able to give the

victims the attention that they need. Staggering of notification will be discussed by CyberScout staff upon receiving notice of a Breach.

c. Does the Company want CyberScout to act as "first call" allowing people receiving notification to contact CyberScout directly? Or does Company want to handle first call, and then send victims into CyberScout ?

This will depend upon the size of Breach and whether the Company opts to offer additional credit products, etc. MOST CLIENTS OPT FOR FIRST CALL BY CyberScout*.*

6. Final review of the Breach notification letter is submitted to CyberScout to make sure that all relevant information such as the toll free number (provided by CyberScout) and description of CyberScoutservices, are accurate.
7. Once the final signoff is granted by both parties, CyberScout will provide the Company with the requisite number of unique "generic" CODES (and, if necessary, and in the case where proactive credit products are offered, PASSWORDS) used for verification purposes.

   CODES and PASSWORDS are generated by CyberScout *and do not contain or utilize any unique identifiers such as Name, SIN, policy number, account number, etc.* The CODES will be provided in either a text file or Excel spreadsheet. The Company uses the codes and connects the unique CODES and PASSWORDS to the victims' names and/or account numbers by a simple mail merge performed by the Company in house or by their mail house/service. CyberScout inputs all CODES and PASSWORDS into CyberScout's systems and activates the unique toll free number (provided by CyberScout for the Company to use) contained in the notification letter prior to mailing.

   NOTE: CyberScout ONLY uses the CODES and PASSWORDS for verification that the caller has received a notification letter and then collects any required information from the victims if and when needed to provide resolution services. **LIKE ALL OF OUR SERVICES THERE IS NO DATA TRANSFER OF THE MEMBER'S PERSONALLY IDENTIFIABLE INFORMATION BETWEEN THE COMPANY AND CYBERSCOUT !!**
8. Once relevant law enforcement, CyberScout, your Company's Legal Counsel and/or leadership have given clearance for providing notification and have signed off and approved the notification letter's content, the Company then mails the notification letters.
9. Company may opt to have CyberScout help in additional media and bureau notification, if necessary, at no additional charge.

   a. At the Company's discretion, CyberScout can work with the Company to issue a press release in conjunction with sending the mailing. Proactive media response is **HIGHLY** recommended in most medium and larger Breaches to minimize the media's and public's reaction and to provide spin control of the incident. This also helps to avoid annoying and unnecessary media calls and inquiries to the Company.
10. CyberScout begins handling victims and distributing any additional credit products opted for by the Company to callers who contact CyberScout.
11. Depending upon the size of the Breach, CyberScout can provide daily, weekly and/or monthly activity reports with call statistics regarding the Breach. These reports may include uptake rates, numbers of data subjects experiencing problems with fraud and identity theft, etc.

a. Reports shall be sent electronically to your Company and will be sent to your Primary Contact.
b. All reports will indicate activity occurring within 24 to 48 hours of the issuance of the report.

Client Company Incident Details

Fill out and E-mail to breach@CyberScout.ca
(In the event that you are unable to send electronically please Fax to 514-360-3701)

Complete By:	
Company Name	
Incident Reference Name (the name that you would like to use to refer to the specific incident)	
Primary Contact Name	
Primary Contact Phone	
Primary Contact E-mail	
Primary Contact Address	
Escalation Contact Name	
Escalation Contact Phone	
Escalation Contact E-mail	
Escalation Contact Address	
Basic Customer Profile	
Number of Affected Individuals	
Discovery Date of Breach	

Fill out and E-mail to breach@CyberScout.ca
(In the event that you are unable to send electronically please Fax to 514-360-3701)

Method of Breach if known (For Example: lost/stolen laptop, lost or stolen backup tape, mis-mailing, etc.)	
States of Domicile/Residence of Affected Data Subjects (if known)	
Type of information Disclosed (Name, Address, D.O.B., SS#, Driver's License Number, etc.)	
Target Date for Notification Letter Mailing	
Client Customer Service Phone Number	
Additional Credit Products that Company wishes to make available to victims of Breach, if any. (Such products are available at an additional charge and may include single bureau credit monitoring, triple bureau monitoring, credit reports, etc.)	
IF ADDITIONAL CREDIT PRODUCTS ARE TO BE OFFERED PLEASE FILL IN THE INFORMATION BELOW	
Billing Contact Name	
Billing Contact Phone	
Billing Contact Email	
Billing Contact Address	

The following pages contain a sample Frequently Asked Question (FAQ) document that can be completed or used as a model by a company that has experienced a breach. This document can then be used by a company's internal staff and to assist CyberScout fraud specialists with the handling of incoming breach calls and questions. This FAQ document is a sample document only. When

contacting CyberScout additional samples that include information on monitoring products and other additional offerings and facts can be provided.

Sample Company FAQs

Refer all media inquiries to the Media Relations Hotline at 1-877-555-1234

XYZ COMPANY FAQs

Refer all media inquiries to the Media Relations Hotline at 1-877-555-1234

1) **What happened?**

In early March, a security incident occurred at a facility operated by a business unit of XYZ. A computer server containing some personal information of individuals who had an account between 2002 and 2008 was stolen

2) **Who is XYZ Company? Why did they have my information?**

XYZ Company is a company that assists with managing promotional offers associated with XYZ members in Vancouver. As part of these processes, we use information necessary to manage the processing of offering special promotional offers. Such information might have included name, address, Social Insurance number, and a date of birth.

3) **Why am I receiving this notification?**

We want you to be aware of this incident because some of your personal information regarding your Vancouver account was stored on the stolen computer server. We're committed to protecting the privacy and personal information of every one of our members. While we have no indication that anyone's personal information has been compromised, we are treating this as a serious situation. XYZ is notifying all potentially impacted PIP members.

4) **I have an account with XYG, why didn't I get a notice?**

Only those people who may be affected by this incident will receive notification.

XYZ Company is working to identify and notify everyone whose personal information was contained on this server. We will make every effort to mail all notices by April 10th.

5) **How might this affect me?**

Some of your personal information was contained in the files that were stored on the stolen computer server. At this time, we have no indication that any of the information that was on the stolen computer server has been misused. The files included, name, address, Social Insurance number and Date of birth.

6) **I never gave you permission to share my personal information.**

As provided in the Privacy Statement, may provide your information to persons or organizations in and outside of as permitted or required by law. For example, we may provide your information to organizations that assist us in offering products and services you may be interested in

7) **What is the status of the stolen computer server?**

Police authorities in Vancouver are conducting an on-going investigation into the stolen computer server. The server has not yet been recovered.

8) **What is XYG doing to assist me?**

Although we have no indication that your information has been misused, we recommend the ongoing educational materials, and resolution service should your information be misused. This service will be provided through CyberScout, a company that specializes in identity theft education and resolution. You can contact CyberScout at 1-866-272-1223. You will be asked to provide the code printed on the letter you received from us. Fraud specialists at the company will assist you in understanding your options with respect to reviewing your credit file, requesting fraud alerts, and notifying appropriate agencies. Additionally, the names, addresses and telephone numbers of both reporting agencies, Equifax Canada and TransUnion of Canada, are included in the letter you have received. Canadian residents have the ability to request free copies of their credit reports as often as needed. CyberScout can help you with any questions you may have about this service.

9) **What will happen if I find out my identity has been stolen?**

At this point, we have no indication that anyone's information is being misused, however we are offering free credit reports, ongoing educational materials, and resolution service as a precaution (credit monitoring services require an internet connection and valid email address). In the unlikely event that your information is misused, a personal advocate will work with you from the first call you make to report the problem until the crisis is resolved. CyberScout will notify the appropriate agencies, businesses, institutions, and create a comprehensive case file for insurance companies and police. In addition, they will follow through on every aspect of the case until your identity has been restored.

10) **Who is** CyberScout**?**

CyberScout is a company that specializes in identity theft education and resolution. XYG has retained them to offer their assistance to you. In the event that your information is misused, they can work with you to help resolve the situation.

11) **Why wasn't I notified sooner?**

As soon as became aware of the situation, we began investigating the incident. We had to work from backup copies of the data. We worked with the data file to determine the names of the individuals whose claim information was stored on the computer server. As soon as possible after the potentially affected persons were identified, notice was sent.

12) **How many people were included in this incident? How many other people's information was stolen?**

Our Company is notifying approximately 75,000 members about this security incident.

13) **How has XYG responded?**

We are very concerned about this matter and are taking appropriate steps to help protect the confidentiality of our members' and members' information. Immediately after learning of the security incident, we conducted an enhanced compliance security review. We have conducted onsite assessments of XYZ Company facilities. We are also working without security staff to implement additional security measures.

14) **What is being done to prevent a similar security breach in the future?**

We have taken several steps to increase the security of the process:
Immediately after learning of the security breach, XYZ Company to implemented additional security measures – including increased physical security and additional security cameras – as added protection for this sensitive data will continue to require vendors to maintain the privacy and security of customer and claimant information.
We are conducting a compliance review of our company's security to determine whether additional measures beyond the controls already being implemented are needed.

15) **This situation has greatly upset me. I want to cancel my accounts with XYZ. Who do I call?**
(We would recommend something like the following: "We value you as a customer and want to assure you we are taking appropriate steps to safeguard your information. We are making available – free of charge – credit reports, ongoing educational materials, and resolution service should your information be misused. If you still wish to cancel your account, you may contact _____ at (555) 555-1212

16) **I represent Mr. XYZ and we're going to file suit. I'd like to talk to one of your attorneys about service of the lawsuit. Can you transfer me to them?**

Refer caller to escalation contact if necessary at:
JANE DOE (123)-555-1212

Breach Reporting Forms

The following page contains links to various reporting forms to provide notification of a breach of private information to the applicable Provincial or Federal privacy authorities. Note that not all provinces and territories have reporting forms, links or requirements:

Office of the Information Privacy Commissioner of Canada:
https://www.priv.gc.ca/resource/pb-avp/pb_form_e.rtf

Office of the Information Privacy Commissioner of Alberta:
https://www.oipc.ab.ca/media/687740/form_breach_report_oct2015_web.docx

Office of the Information Privacy Commissioner of British Columbia:
https://www.oipc.bc.ca/tools-guidance/forms/online-privacy-breach-report-form/

Office of the Information Privacy Commissioner of Manitoba:
https://www.ombudsman.mb.ca/uploads/document/files/reporting-a-privacy-breach-to-manitoba-ombudsman-march-2007-en-1.pdf

Notification Communications

Notification to impacted individual can take a number of different forms ranging from letters and E-mails to public disclosure to the media to publishing on social media and the company website. The form of the communications should be that which is most reasonably likely to reach the individual(s) impacted by the incident.

The content should at least provide the following pieces of information:

- Date of the breach;
- Description of the breach;
- Description of the information inappropriately accessed, collected, used or disclosed;
- Risk(s) to the individual caused by the breach;
- The steps taken so far to control or reduce the harm;
- Future steps planned to prevent further privacy breaches;
- Steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch, information explaining how to change a personal health number or driver's licence number);
- Contact information of an individual within the organization who can answer questions or provide further information;
- Privacy Commissioner contact information and the fact that individuals have a right to complain to the Office of the Information and Privacy Commissioner. If the public body or organization has already contacted the Privacy Commissioner, include this detail in the notification letter.

As noted above, the breach notification letter should include a contact number within the organization in case affected individuals have further questions.