Oregon Consumer Identity Theft Protection Act (SB 583)
Notification Best Practices

Agency Notification Best Practices

Agencies are entrusted with many varieties of sensitive and confidential information. This includes the personal information of a variety of consumers including clients, customers, licensees and employees. As owners and custodians of that information, agencies are responsible for protecting those assets from loss or misuse.

The Oregon Consumer Identity Theft Protection Act (SB 583) outlines steps to take when there is a security breach of personal information. The Department of Administrative Services offers best practices to consider as agencies implement the required security breach notification provisions of the Oregon Consumer Identity Theft Protection Act.

The best practices incorporate industry best practices and the requirements of the Oregon Consumer Identity Theft Protection Act.

Definition of Personal Information:

A consumer's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or data elements are not encrypted or when the data elements are encrypted and the encryption key also has been acquired, or when either the name or the data elements are not redacted:

A. Social Security number
B. Driver's license number or state identification card number
C. Identification number issued by a foreign nation
D. Passport number or other United States issued identification number
E. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account.

This means any of the data elements or any combination of the data elements listed above when not in connection with the consumer's first name or first initial and last name, if the information if compromised would be sufficient to permit an individual to fraudulently assume or attempt to assume the identity of the consumer whose information was compromised.

Agency Security Breach Notification Best Practices Checklist

1.0	Establish a process for assessing whether a breach notice is either legally mandated or otherwise appropriate	Required	Optional	N/A
1.1	Establish a breach notice group or designate an individual tasked with assessing, in case of a breach, whether the need for a breach notice has been triggered and, if so, carrying out the breach notice process. If assigned to an individual, designate a substitute in case of vacation, illness or absence for any reason.			
1.2	Identify and determine if state breach notice and other privacy-related laws, as well as any relevant Federal laws are applicable. Such laws mandate, under certain circumstances, notifying individuals whose personally identifiable information has been accessed or acquired in an unauthorized fashion. Factors impacting such legal requirements will include the nature of a breach, the type of information involved, and the jurisdictions impacted.			
1.3	Establish a process for determining whether notice is legally mandated or otherwise appropriate.			

2.0	Suspected ID Theft	Required	Optional	N/A
2.1	Conduct an investigation. • Determine severity and scale of potential or actual harm • Determine seriousness of any potential breach of the law • Identify immediate and underlying causes and the lessons to be learned • Prevent recurrence • Take appropriate action, including formal enforcement			
2.2	Delay notification if law enforcement agency determines that the notification will impede a criminal investigation and agency has made a written request that the notification be delayed.			
2.3	If, after consultation with relevant federal, state or local agencies responsible for law enforcement, it is determined that no reasonable likelihood of harm to the consumers whose personal information has been acquired has resulted or will result from the breach: • Document in writing • Retain for 5 years			

3.0	Confirmed ID Theft	Required	Optional	N/A
3.1	Conduct a risk assessment that determines: • the impact • the confidential information involved • if the confidential information can be compromised (was the information adequately encrypted – more than just password protected)			

	• how many potential victims are affected • who are the potential victims affected • how public the event is – was it internal or external, intentional or unintentional • the level of risk and then decide if there is a need to contact potential victims (err on the side of caution)			
3.2	Create an internal response team with the expertise, authority, and resources to act quickly in case of a security incident. Consider including representatives from these departments: information technology, security, privacy, legal, marketing/sales/customer relations (in case customer data is involved), human resources (in case employee data is involved), and media relations. The team may also include outside experts under retainer or contract.			
3.3	Prepare a notification letter to send to potential victims (see attached sample)			
3.4	Set up or use an existing toll free number for potential victims to call – train staff how to respond to callers. Expect about 15% to 20 % of potential victims to call.			
3.5	Develop a list of frequently asked questions and post them on the agency Web site (see attached sample of potential questions)			
3.6	Depending on the level of risk, determine the need to offer potential victims a credit monitoring service (generally for 6 months to a year)			

4.0	**Establish a process for determining who to notify once the need for a breach notice has been triggered.**	**Required**	**Optional**	**N/A**
4.1	Determine who has been affected and notify each affected individual when possible. Double-check the list of recipients before sending.			
4.2	Determine proper notification medium: • Written • Electronic if this is the person's customary method of communication • Telephone, provided that the contact is made directly with the affected consumer • Substitute notice if an agency can demonstrate that the cost of providing notice would exceed $250,000, that the affected class of consumers to be notified exceeds 350,000, or if the agency does not have sufficient contact information to provide notice. Substitute notice consists of the following: o Conspicuous post of the notice or a link to the notice on the Internet home page of the agency if the agency maintains one; and o Notification to major statewide television and newspaper media.			
4.3	Try to ensure that only those individuals whose personally identifiable information was compromised are included in the group to be notified. If you cannot determine the exact individuals affected, consider notifying all members of the group affected if the likelihood of material harm outweighs the uncertainty that the individuals were affected.			

5.0	Establish a process for communicating a breach notice.	Required	Optional	N/A
5.1	Consider potential communication channels for different circumstances, e.g., your plan may be different for an employee as opposed to a customer data breach. • Your human resources office • Agency Public Information Officer (PIO) • DAS Director's Office – 503-378-3104 • DAS Office Communication Manager – 503-378-2627 • State Chief Information Security Officer – 503-378-6557 • Department of Justice • Oregon State Police – 503-378-3720 (ask for the Criminal Lieutenant) • Other agencies that may be affected • If security breach affects more than 1,000 consumers, contact all major consumer-reporting agencies that compile and maintain reports on consumers on a nationwide basis; inform them of the timing, distribution and content of the notification given to the consumers. • Contact the credit monitoring bureaus in advance if directing potential victims to call them o Equifax – 1-800-525-6285 o Experian – 1-888-397-3742 o TransUnion – 1-800-680-7289			

6.0	Considerations that affect the timing of a breach notice	Required	Optional	N/A
6.1	In general, notify affected individuals as soon as reasonably possible after a breach is discovered, unless law enforcement officials indicate that notice would impede their investigation.			
6.2	If you have reported the breach to law enforcement, ask them to inform you when it is safe to notify affected individuals. Send out notice as soon as practicable and in compliance with existing notification laws when so informed. Consider appointing a member of the response team to follow up with law enforcement in order to find out when it is safe to notify the affected individuals. When possible, get such confirmation in writing.			
6.3	Send the notification in an appropriate manner to the intended audience. In consumer notification cases, consider notice by traditional mail and by email where appropriate.			
6.4	Consider the option of giving general public notice on the agency Web site and/or through major media, where the group to be notified is very large or it is otherwise appropriate			

7.0	Educate and coordinate with your own and other potential resources	Required	Optional	N/A
7.1	Educate your staff or other customer service employees about the breach so			

	they can provide knowledgeable assistance. Consider having assistance available evenings and weekends.			
7.2	If the breach involves financial information, consider notifying credit reporting agencies before sending out notice of a breach to a large number of individuals, so they can prepare for the consequent inquiries. (You will find information about the major Credit Reporting Agencies at www.ftc.gov/bcp/conline/edcams/gettingcredit/faqs.html.) However, do not delay notice to individuals because of cooperation with credit reporting agencies.			

8.0	**Content of breach notice communication.**	**Required**	**Optional**	**N/A**
8.1	Consider carefully the content of any breach notice communications and focus on providing the most useful information possible.			
8.2	In the case of consumer breach, notification should include: • The date of the breach • The information accessed • Description of the incident in general terms • Contact information • Contact information for national consumer reporting agencies • Advice to the consumer to report suspected identity theft to law enforcement, including the Federal Trade Commission.			
8.3	Consider available options should you not have complete contact information for all impacted individuals: • Written • Electronic if this is the person's customary method of communication • Telephone, provided that the contact is made directly with the affected consumer • Substitute notice, if an agency can demonstrate that the cost of providing notice would exceed $250,000, that the affected class of consumers to be notified exceeds 350,000, or if the agency does not have sufficient contact information to provide notice. Substitute notice consists of the following: o Conspicuous post of the notice or a link to the notice on the Internet home page of the agency if the agency maintains one; and o Notification to major statewide television and newspaper media.			
8.4	Consider providing further information that might be helpful for those who believe they maybe a victim of identity theft. For example, include a brochure about how to set up credit monitoring or how to read a credit report could be helpful. Information is available from the Federal Trade Commission (www.ftc.gov/bcp/menus/consumer/data/idt.shtm).			
8.5	Consider offering free credit monitoring services for one year to affected individuals, particularly if the incident involved Social Security or driver's license numbers. When considering making such an offer, note that often			

	only about 25% of consumers will accept such an offer.			
8.6	Consider providing links on your Web site to resources such as the following: • The three major credit reporting agencies (available at the Federal Trade Commission Web site www.ftc.gov/bcp/conline/edcams/gettingcredit/faqs.html) • Government agency resources such as this Federal Trade Commission identity theft consumer alert (www.ftc.gov/bcp/conline/pubs/alerts/infocompalrt.htm) • Identity Theft Resource Center (www.idtheftcenter.org) • Privacy Rights Clearinghouse (www.privacyrights.org).			

9.0	**Follow Up**	**Required**	**Optional**	**N/A**
9.1	Track phone calls received from those who were notified			
9.2	Track those who are registering for credit monitoring (if offered)			
9.3	De-brief with those involved in coordinating/managing the incident			
9.4	Document lessons learned			
9.5	Address security issues causing the incident			
9.6	Update the agency information security plan			

ID Theft Sample Notification Letter

NOTE: This is offered as an example, <u>not</u> a template.

DATE

Important information about your confidential information

On (date), computer security staff at the (Agency Name) found (describe incident). According to the best information available from our staff and computer experts at the Oregon State Police, we believe that your (describe personal information that may have been compromised). We have identified (number of citizens) whose information is affected and we are researching information from (number) additional citizens to see if their information is affected.

We are diligent about protecting confidential citizen information and deeply regret that our safeguards did not work in this instance. We are reviewing our security practices and procedures to further strengthen our protection for all confidential citizen information.

I am enclosing information about identity theft written by the Federal Trade Commission. I encourage you to monitor your personal information relating to recent financial transactions. If you notice any suspicious activity on your statements, you should report it immediately to the financial institution involved and contact the Federal Trade Commission at www.consumer.gov/idtheft or at 1-877-ID-THEFT (438-4338).

(Include information on credit monitoring services – for example: For more information, please call 1-800-xxx-xxxx toll-free from an Oregon prefix or xxx-xxx-xxxx (outside Oregon). Choose the language option, then choose option "5" to speak with a representative. If you get a busy signal, please call our message line at xxx-xxx-xxxx and leave your name and phone number and we will return your call within four hours. You may also e-mail us at questions. (agency e-mail address).)

TTY (hearing or speech impaired; machine only): xxx-xxx-xxxx (city) or 1-800-xxx-xxxx (toll-free from Oregon prefix). **Americans with Disabilities Act (ADA):** This information is available in alternative formats. Call xxx-xxx-xxxx (city) or 1-800-xxx-xxxx (toll-free from Oregon prefix). **Asistencia en español.** Llame al xxx-xxx-xxxx en (city) o llame gratis de prefijo de Oregon al 1-800-xxx-xxxx.

Thank you.

(Agency Director Name), Director
(Agency Name)

ID Theft Credit Monitoring Template Letter

NOTE: This is offered as an example, <u>not</u> a template.

DATE

Free Credit Monitoring for Citizens Affected by Illegal Software Intrusion

Recently, the (Agency Name) experienced its worst nightmare – some citizen personal information was (describe incident) Your personal information was included. Earlier this month, we sent you a letter explaining what happened. We also posted Frequently Asked Questions (FAQs) on our Web site, (agency's Web site). To date, we have had no reports of identity theft as a result of this incident. However, to protect your information from possible fraud, we are offering credit monitoring and restoration services at no charge to affected taxpayers.

We have contracted with (name of company and what services they offer).

Here's how it works:

- If you choose to enroll, you must contact (company name) directly.
- ***We will not provide Identity Safeguards with any information about you*** other than to confirm that you are eligible to receive this free service**.**
- Once you enroll, you will receive a copy of your credit report, regular updates on credit activity, and credit restoration if your information is used fraudulently.

Please see the enrollment instructions on the back of this letter so you can begin your protection with (company name). If you have questions about the incident or want more information, please call the (Agency Name and 1-800 number) (toll-free from an Oregon prefix) or xxx-xxx-xxxx (Salem area and outside Oregon). If you get a busy signal, please call (xxx-xxx-xxxx) and leave your name and phone number—we will return your call within four hours.

Since this incident, we have taken further steps to protect all confidential citizen information. I regret this security intrusion. I encourage you to enroll in (company's name) program to protect your information. Please don't hesitate to call us at one of the numbers above if you have questions. Thank you.

Sincerely,

(Agency Director Name), Director
Name of Agency

Take These Steps to Protect Your Identity and Credit

By taking the following three steps **right now**, you can help protect your identity and credit from fraud. It will take 20 to 30 minutes to complete this process.

Step 1: Enroll in (company's name) protection services for 12 months. The (Name of Agency) is paying for this service so there is no cost to you. ***To enroll in this pre-paid service, (include information on how to sign up for services).***

If you have any questions, please contact (company's name and contact number) or call the (Agency Name), 1-800-xxx-xxxx (toll-free from an Oregon prefix) or xxx-xxx-xxxx (city area and outside Oregon). If you get a busy signal, please call xxx-xxx-xxxx and leave your name and phone number – we will return your call within four hours.

After you enroll, (describe what will happen – next steps). The information describes its services and the next steps you'll need to take to help protect your good name.

Step 2: Activate the credit monitoring service provided.
You will receive instructions on the credit monitoring service when you enroll (Step 1). Once you start this service, you will receive weekly credit reports that will alert you to any unauthorized changes to your credit. This service is included with your pre-paid membership, ***but you must activate it.***

If you notice any suspicious activity on your weekly credit report, immediately report it to (company name). A recovery advocate will work with you to assess, stop, and reverse any damage to your identity. The (Agency Name) is also paying for this service.

Step 3. Place a fraud alert at one of the three major credit bureaus via the internet or by phone. We encourage you to do this even if you are not aware of any suspicious activity. You do not need to enroll with Identity Safeguards to place this alert yourself.

A fraud alert will prevent someone from opening new financial or credit accounts in your name. As soon as one credit bureau confirms your fraud alert, the others are notified and will also place fraud alerts.

You may contact any of the credit bureaus through the Internet or by telephone:

- **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

All three companies will mail you free copies of your credit reports.

If you choose to enroll in the (company's name) program and need help contacting the credit bureaus they can help you do that at no charge.

Sample FAQ

Frequently Asked Questions

- I received your letter but I am not sure exactly what it means?
- How do I know whether I am affected?
- Why did you even have my personal information?
- Does this mean I am the victim of identify theft?
- What are you going to do about this?
- How can I protect myself from identity theft?
- Why can't I get through to the credit bureau to place my fraud alert?
- What should I look for in my credit report?
- What if there's a problem on my credit report?
- What do I do if I am a victim of identity theft?
- Will a fraud alert prevent me from using my credit cards or getting new ones?
- Can I put a freeze on my credit report so that it is not sent to other people?
- Will the State pay for credit monitoring?
- Is it OK to give my Social Security number to the credit bureau fraud line?
- Should I change my Social Security number?
- Will the state contact me to ask for personal information because of this event?

NOTE: This list is offered as potential questions agencies will want to consider using on a Frequently Asked Questions notice or posting. The actual answers to these questions will, in many cases, be agency-specific. General questions and answers about identity theft can be found at the Federal Trade Commission site at www.consumer.gov/idtheft.