

PRICE WATERHOUSE COOPERS

SECURITY BREACH FACT SHEET

**FOR DEPARTMENT OF ADMINISTRATION
CALL CENTER**

Who is affected by the breach?

Participants in the Public Employees Retirement System and the Teachers Retirement System, who were active or inactive employees, including retirees, in 2003 and 2004. If you are affected by this breach, you will be mailed a notice shortly with more detailed information about the breach, and instructions on how to sign up for free services pursuant to the settlement reached with PwC.

What information was lost?

The lost information contains names, social security numbers and dates of birth.

What should I do now?

You will receive a notice in the next few weeks that describes the protections PwC has agreed to provide to affected Alaskans. This will include free credit monitoring and identity theft protection, or placing a security freeze on your credit report. Details about what these protections entail and how you can sign up for them will be explained in the notice. The notice will also explain how you can make a claim for any damages you may incur if you become an identity theft victim.

In the meantime, there are other steps you can take to protect yourself against identity theft:

1. You can place a fraud alert on your credit report, even if you have credit monitoring in place. You can contact the three main credit reporting agencies below to place a fraud alert:

Equifax	1-888-766-0008	www.equifax.com
Experian	1-888-397-3742	www.experian.com
TransUnion	1-800-680-7289	www.transunion.com

A fraud alert will not prevent access to your credit report, but it will alert the reporting agency, and businesses checking on your credit, that your information has been compromised. If you have already placed a security freeze on your credit report, a fraud alert is not necessary.

2. Get a copy of your credit report and review it for suspicious activity. Under federal law, you are entitled to a free copy of your credit report from each of the three credit bureaus every year. To get your free copy, contact each of the credit agencies listed above, or go to www.annualcreditreport.com. Look for any accounts you do not recognize, and cancel them immediately.
3. Account monitoring. Check your monthly account statements carefully for suspicious charges, and notify your financial institution of all charges you do not recognize. Close any accounts that you think have been compromised.
4. Consumer Education. There are several consumer resources available that provide valuable information on identity theft, and how to avoid becoming a victim. The Federal Trade Commission maintains a website that contains a wealth of information on identity theft at www.ftc.gov/idtheft.

Has my information been misused?

There is no indication that any of the missing information has been misused, and we have not received any reports of identity theft that can be related to this breach. But you should take precautions to guard against the possibility that your personal information may fall into the hands of an identity thief.

What are you doing now to protect my personal information?

This breach resulted from actions by a private company hired by one of the state's contractors. The state is continually upgrading and revising policies to address the ever changing demands on information security. The state implements security protocols aimed at protecting the personal information it receives from Alaska citizens. These actions include advanced firewalls and computer access restrictions to prevent unauthorized access to the state's electronic data; encryption requirements for data and information transmission; security requirements that restrict access to state offices by unauthorized personnel; and other requirements to ensure the state's confidential data and information is secure.

Does PwC still have my information?

Yes. PwC may still need this information in connection with the litigation we have filed against Mercer. However, PwC is aware that this information must be protected, and has taken every precaution to ensure it is not compromised. As soon as PwC does not need the information for any legitimate purpose, it will be destroyed or returned to the state.

Is my retirement affected?

No.

What are some of the things someone can do with my personal information?

Identity theft occurs in many forms. Here are some of the common ways identity thieves can misuse your information:

New account fraud: This happens when an identity thief uses your personal information to open up new accounts in your name, but will use a different address. Thus, you may not discover the new account for some time.

Existing account fraud: This occurs when an imposter uses your current account information to commit fraud. You can learn of this kind of fraud by reviewing your monthly account statements.

Debit or check card fraud: This occurs when a thief uses your debit or check card to remove money from your bank account. This is sometimes prevented if your accounts can only be accessed with a PIN, but there are ways to avoid this by making “off line” transactions.

Social Security number fraud: This happens when an imposter uses your SSN to gain employment, for tax reporting purposes, or other illegal transactions.

Criminal Identity Theft: This occurs when a criminal gives another person’s name and personal information during an arrest. If the imposter then fails to appear in court, an arrest warrant can be issued with your name on it!

You can get information about these kinds of identity theft from several online resources, including the FTC’s web site, www.ftc.gov/idtheft.

What’s the difference between credit monitoring, identity theft protection, and a security freeze?

There is a significant difference between these:

1. “Credit monitoring” can be done on your own by regularly checking your credit reports for suspicious activity. There are also a number of services that will do this for you on a daily or weekly basis for a fee. If suspicious activity occurs, you are generally notified immediately via email. This will allow you to take action to close accounts that are not yours, and notify creditors that someone is using your name illegally. Credit monitoring will not prevent this kind of “new account” identity theft, but it will alert you promptly to the illegal conduct.
2. “Identity theft protection” is a service offered by several companies that provides insurance in the event you become a victim of identity theft. This is often offered in connection with credit monitoring services. Depending on the type of protection, it can reimburse you for damages you may suffer as a result of identity theft, and assist you in repairing your credit.
3. A “security freeze” locks your credit files at the three credit reporting agencies until you unlock your file with a password or PIN. In Alaska, this freeze can cost you up to \$5 for each credit reporting agency. A freeze stops new accounts from being established by imposters. However, a security freeze will not stop misuse of existing bank or credit accounts, or some other kinds of identity theft. A security freeze will also prevent you from engaging in any transactions that require checking your credit report. You can request access to your credit report when a freeze is in place if you provide you PIN, and pay a \$2 fee. You should consider the frequency with which you need access to your credit report before you decide to place a security freeze on you accounts.

What happens if I become a victim of identity theft?

The settlement we reached with PwC contains provisions that will likely reimburse you for damages you sustain if you become a victim of identity theft as a result of this breach. To get this protection, you will need to sign up for credit monitoring and identity theft protection under the terms of the settlement. More details about how to do this, and how to make a claim for damages, will be explained in the notice you will receive in a few weeks.

How was the information lost?

It is still unclear exactly how the information was lost. PwC kept the information in its office in Chicago. PwC discovered the information was missing in December.

Background – how did PwC get this information?

For many years, an actuarial firm was contracted by the state to perform actuarial services for the Department of Administration (“DOA”). The DOA would routinely provide the firm with information on current and former state employees that allowed the firm to predict the state’s retirement obligations, and to calculate PERS and TRS pension and health care rates. As part of litigation against the firm, Price Waterhouse-Coopers LLC (PwC) was given information on Alaska retirees held by the actuary firm, including the confidential personal information that was subject to this breach.