2/11/10 OVERVIEW: SECURITY BREACH PERSONAL INFO...

SUMMARY OF STATE'S AGREEMENT WITH PRICEWATERHOUSE COOPERS LLP

- PricewaterhouseCoopers (PwC) has accepted responsibility for the loss of data.
- PwC has agreed to provide at least two years of credit monitoring and I.D theft protection OR a security freeze and adjustments to the security freeze (up to a total of $33) for each affected consumer.
- The identity theft protection and credit monitoring service may be extended for one year if there is evidence of identity theft from this loss of confidential data; if there is further evidence in the third year, the State and PwC may decide to extend for an additional period of time.
- PwC will establish a call support center that will enroll affected participants in the service they choose and provide credit counseling
- Consumer reimbursement. PwC will reimburse consumers for losses suffered as a result of identity theft caused by this breach. If an affected participant suffers damages from ID theft, the participant can submit a claim to PwC in arbitration. If the participant has enrolled in one of the options (identity theft protection and credit monitoring service or security freeze), they will get a rebuttable presumption that the ID theft was the result of PwC's loss of the confidential data.
- PwC will pay up to $100,000 to the State for notices to each affected participant.
- PwC will indemnify the State for any claims made against the state related to this incident.
- The settlement does not release any individual consumer claims. Each affected consumer can pursue any claims they may have against PwC.

PRICE WATERHOUSE COOPERS

SECURITY BREACH FACT SHEET

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.

To Request your Credit Report by Phone:

Call 1-877-322-8228. You will go through a simple verification process over the phone.

Will credit monitoring or a credit freeze affect my credit score?

No. You have the right to monitor your credit without it affecting your credit score. If you request your own credit report it has no affect on your credit score. Placing a security freeze will also not affect your credit score, but it will prevent any activity -- both good and bad-- on your credit file.

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 retirement plan participants held by the actuary firm, including the confidential personal information that was subject to this breach.

Don Habeger

From: [redacted]
Sent: Wednesday, February 10, 2010 11:39 AM
To: Rep. Jay Ramras
Cc: [redacted]
Subject: Missing Personnel Records

Dear Representative Ramras,

My good friend, Bob Roses, suggested that I contact you and the other members of the Judiciary Committee concerning the State's responsibility for the missing employee and retiree information.

I am Tom E. Main, a 63-year resident of Alaska and a PERS retiree with 32 years State service and am retired under Tier I. I am presently in Southern California because my wife is receiving medical care. My phone number is [redacted]

Bob Roses told me that the Judiciary Committee was holding either a Hearing or a Discussion today (2/10/2010) with the State Department of Administration concerning the lost records.

The State is telling those employees/retirees that it is their responsibility to take whatever action is necessary to protect themselves from Identity Theft. I disagree.

I believe it is the State that erred and it is the State's responsibility to do whatever is necessary to protect the affected personnel. The State could contract with a Credit Monitor and ID Insurance provider much more easily than can 77,000 individual employees. In this case, I recommend that the State contract with a Credit Bureau and not a "sub-contractor".

I have the following questions:

1. Why did the State provide Mercer with Full Name, SSN, and Date of Birth when the actuarial analysis would need only Sex, Age, Years of Service and Tier?

2. The State recommends that the affected personnel invoke a Fraud Alert with the Credit Bureaus. A Fraud Alert is good for 90 days and can be extended for an additional 90 days.

Until the missing information is found and proven not to have been compromised, the personnel are at risk ad infinitum----maybe for the rest of their lives.

If the personnel must provide their own security, a Credit Freeze can be implemented for several years, but this requires validation by a police report. Are the Alaska State Troopers or other law enforcement agency going to provide 77,000 employees/retirees with such reports? A Credit Freeze is extremely inconvenient to the personnel involved. Their whole access to credit is affected.

3. I provided a Survivor's Benefit for my wife. Was her personal information also lost?

4. If the personnel do have to provide their own security, how do they get reimbursement for the cost (maybe forever).

5. The SECURITY BREACH FACT SHEET states, "The settlement we reached with PwC contains provisions that will likely (emphasis added) reimburse you for damages you sustain*****"

Just what is meant by "likely".

What about time and inconvenience experienced by personnel because of the State's mistake?

What if PwC discovers that the cost is so great that they file for bankruptcy?

6. Is this the only information that is lost? E. g. If you have a direct deposit, was the Bank Account Number also lost?

7. With only the name, SSN, and age, a person's bank accounts and other personal accounts, information, etc. could be breached. How are we to protect ourselves from this?

Any assistance that you or the Judiciary Committee can provide will be appreciated.

Sincerely,

Tom E. Main

STATE OF ALASKA

DEPARTMENT OF ADMINISTRATION

ANNETTE KREITZER, COMMISSIONER

SEAN PARNELL, GOVERNOR

P.O. BOX 110200
JUNEAU, ALASKA 99811-0200
PHONE: (907) 465-2200
FAX: (907) 465-2135

March 11, 2010

The Hon. Jay Ramras, Chairman
House Judiciary Committee
Alaska House of Representatives
State Capitol, Room 120
Juneau, Alaska 99801

Dear Representative Ramras:

The purpose of this letter is to provide an update to the testimony Deputy Commissioner Kevin Brooks offered during the February 11 House Judiciary Committee hearing regarding the security breach by Price Waterhouse Coopers (PwC) and to address the Committee's question about how the Department of Administration (Department), and specifically, the Division of Retirement and Benefits (DRB) plans to keep personally identifiable information secure in the future. The Department remains engaged in remediation of possible effects of the past event, and vigilant to prevent a similar future occurrence.

On February 12, 2010 more than 77,000 PERS and TRS members and former members affected by the PwC security breach were mailed a letter articulating the situation and including information about how to avail themselves of identity theft protections offered through the State's settlement with PwC. To date:

- Affected members have received information through mail notification;
- Over 16,800 members have signed up for an Equifax product;
- Some members (including State employees) have received additional emails and union newsletters;
- DRB answered over 7,000 phone calls regarding the event, to obtain information or to seek assistance in taking advantage of the negotiated settlement protections. Currently, the call volume is much lower – less than 10 per day and declining.
- Retirees will receive a reminder in DRB's quarterly newsletter to verify whether or not their information was affected and to avail themselves of identity theft protections provided by the settlement.

Additional communication tools that will be used to keep PERS and TRS employers and members informed include:

1. Annual PERS and TRS statements from DRB;
2. Quarterly PERS and TRS Newsletters from DRB;
3. Periodic envelope stuffers with benefit checks and advices;
4. Periodic emails to active State employees from DRB;
5. Periodic email newsletter, The Employer's Edge, to all PERS and TRS employers from DRB. Employers often forward pertinent information to their employees;
6. Quarterly account statements, with other investment and retirement information from the State's record keeper Great West Financial Services; and
7. Confirmation of password and investment change from Great West Financial services.

The Department takes very seriously its responsibility to protect individual's personally identifiable information. Currently, DRB protects personally identifiable information by securing the data behind firewalls, in multiple secured locations. Data flowing outside of DRB's system is encrypted using multiple tools designed for specific types of data transfer (file, internet, email, etc.). DRB uses a 'defense in depth' strategy. The State Security Office continuously monitors all DRB systems for network attacks, intrusion detection/prevention, and injection attacks. The DRB Information Systems Section ensures application security is properly implemented by using multi-tiered authentication and access control systems.

DRB is working to add additional "depth" to its security strategy by moving legacy applications under the myAlaska authentication layer by December of 2011. All new applications moved into production will use the myAlaska authentication layer as part of their standard architecture. Additionally, DRB is examining under what circumstances personally identifiable information is released to other agencies or third parties. Data flowing to our business associates, such as our actuary, is being examined to ensure compliance with statutes and to ensure there is a true business need for transferring any sensitive data. The Division recently turned down a request for information that included personally identifiable information from auditors working on behalf of another State department. DRB personnel are becoming very comfortable challenging the business need for this kind of information.

Please contact me if you or the Committee would like additional information.

Sincerely,

Annette Kreitzer