



Handwritten initials

RECEIVED

VIA OVERNIGHT COURIER

'09 JAN -8 AM 11:42

Hawaii Department of Commerce and Consumer Affairs
Office of Consumer Protection
235 S. Beretania Street, Room 801
Honolulu, HI 96813

STATE OF HAWAII
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS

January 6, 2009

Re: Notification of Potential Data Breach

Dear Sirs,

On Monday, December 1, 2008, North Pacific Group discovered that several laptops and other computer equipment belonging to our Human Resources and Information Technology departments in Portland, Oregon had been stolen sometime over the long Thanksgiving weekend.

Since the incident, we have examined all information stored on these computers, searching for sensitive data about our employees, customers, vendors and our business. As a result, we found that two of the stolen computers stored files containing names, addresses, Social Security numbers, and dates of birth for current and certain former employees ("Employees"). Our records indicate that the stolen computers contained such records for over 1,000 Employees, two of whom are located in your State. These records are in hidden locations on these computers and are password protected.

We immediately reported this incident to our local law enforcement authorities, and are continuing to assist in their investigation. We are concurrently sending a written notice to the affected Employees in your State, a sample of which is enclosed. As you will see, the notice outlines the credit monitoring and other services we are offering Employees. We have also contacted the three national credit repositories—Equifax, Experian, and TransUnion—to advise them of the incident.

If you have any questions regarding this incident, please contact me at (503) 230-2105 or our legal counsel, Merrill Baumann of the Dunn Carney firm, at (503) 242-9620.

Sincerely,

Tacy A. Lind
Senior Vice President of Human Resources
North Pacific

Enclosure

cc: Merrill Baumann, Esq.



Secure Processing Center | 600 Satellite Blvd | Suwanee, GA 30024

URGENT — Please Open Immediately.

<FirstName> <MiddleInitial> <LastName> <Suffix>
<Address> (Line 1)
<Address> (Line 2)
<City> <State> <Zip>
<POSTNET BARCODE>



<FirstName> <MiddleInitial> <LastName> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-XXX-XXXX
8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday
if you have questions or feel you may have an identity theft issue,
please call ID TheftSmart member services

Dear <FirstName> <MiddleInitial> <LastName> <Suffix>,

On Monday, December 1, 2008, we discovered that several laptops and other computer equipment belonging to our Human Resources and Information Technology departments in Portland, Oregon had been stolen sometime during Friday evening.

Since the incident, we have examined all information stored on these computers, searching for sensitive data about our employees, customers, vendors and our business. As a result, we found that two of the stolen computers stored files containing names, addresses, Social Security numbers, and dates of birth for current and certain former employees. These files are in hidden locations on these computers and are password protected.

Although we have no reason to believe that this information has been improperly accessed or misused, we want to make you aware of the incident and the steps we have taken to guard against potential identity fraud.

First, we filed a police report with our local law enforcement and notified building security. We are regularly requesting updated information on their investigations. We contacted regulatory authorities and the three national credit repositories—Equifax, Experian, and TransUnion—to advise them of the incident.

Because securing your personal information is so important to us, North Pacific has engaged Kroll Inc., the world's leading risk consulting company, to provide its ID TheftSmart™ service. Kroll's Fraud Solutions team has more experience than any other organization when it comes to helping people who have experienced the unintentional exposure of confidential data. We are providing you FREE access to:

- › **Current Credit Report.** Kroll offers you access to an up-to-date credit report from Experian. If you suspect fraudulent activity, please call the Kroll team
- › **Continuous Credit Monitoring.** Monitoring alerts make you aware of key changes, using data from all three major national credit repositories, in your credit file that could indicate the kind of unauthorized activity commonly associated with identity theft and fraud. *Consumer Credit Report and Credit Monitoring Authorization Form required.*
- › **Enhanced Identity Theft Restoration.** Licensed Investigators who truly understand the problems surrounding identity theft will help restore your name and credit if either should be affected by this incident. The investigators do most of the work!

You may call 1-800-XXX-XXXX, 8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday, if you have any questions or feel you may have an identity theft issue.

Please know that your privacy is of the utmost importance to us. We truly apologize for any inconvenience this incident may cause you and are currently evaluating and implementing steps to prevent a similar occurrence.

Sincerely,

Tracy A. Lind
Senior Vice President of Human Resources
North Pacific