Delivering on A promise.℠

Dead River Company

March 22, 2013

Attorney General Michael A. Delaney
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Dead River Company – Notice of Data Security Event

Dear Attorney General Michael Delaney:

We are writing to notify you of a data event that may have compromised the security of two hundred (200) New Hampshire residents' personal information. Dead River Company ("Dead River"), 82 Running Hill, Suite 400, South Portland, ME 04106, is informing your office of pertinent facts that are known at this time related to the March 6, 2013 detection of malware on Dead River's computer network. This malware may have resulted in unauthorized access by unknown individuals to the personal information of certain Dead River employees, Dead River customers and credit approval applicants. Upon detection of the malware, Dead River immediately commenced an internal investigation into the detection. Dead River retained third-party computer forensic experts Kroll Advisory Solutions ("Kroll") to assist in its identification, isolation, and removal of the malware from its network, as well as the identification of what information on Dead River's network, if any, was at risk as a result of the malware. *On March 8, 2013, Dead River* disconnected its network from the Internet thereby ending the exposure. Dead River retained privacy and data security legal counsel to assist in the ongoing investigation of, and response to, the incident.

Nature of the Data Security Event

On March 6, 2013, Dead River detected the presence of malware on its computer network. Dead River immediately commenced an investigation into the detection, and retained third-party computer forensic experts Kroll Advisory Solutions ("Kroll") to assist in its identification, isolation, and removal of the malware from its network. Dead River also retained Kroll to assist in the identification of what information on Dead River's network, if any, was at risk as a result of the malware. Although this investigation is ongoing, it appears that the personal information of Dead River customers who, on or between March 6, 2013 and March 8, 2013, provided debit card, credit card, or other financial account information, either in person or over the phone, to a Dead River customer service representative who then typed the information directly into a web browser to facilitate account payment or charge-approval privileges, may be at risk as a result of the malware. It also appears that credit approval applicants that provided, either in person or over the phone, their names, dates of birth, and Social Security numbers to Dead River customer service representatives for purposes of applying to receive credit approval may be at risk as a result of the malware. Lastly, the personal information of any Dead River employee using a company web browser to conduct personal or company online business that required the employee to manually input his/her Social Security number, driver's license or state identification card number, or bank account, credit or debit card information, may be at risk as a result of the malware. At this time, Dead River is unaware of any actual or attempted misuse of personal information.

Notice to New Hampshire Residents

Although the investigation is ongoing, it appears that the personal information of two hundred (200) New Hampshire residents may be at risk as a result of the malware. One hundred and ninety-five (200) of these state residents are current Dead River customers and employees, and will be sent written notice of the data security event on or around March 29, 2013 in substantially the same form as the sample notice attached to this letter as **Exhibit A.** On March 18, 2013, Dead River distributed pre-notification internally to all Dead River employees in substantially the same form as the sample correspondence attached to this letter as **Exhibit B.** On March 19 and 20, 2013, Dead River sent pre-notification to the potentially affected customers in substantially the same form as the sample correspondence attached to this letter as **Exhibit C**.

Other Steps Taken/To Be Taken

As discussed above, Dead River retained independent, third-party computer forensic experts and privacy and data security legal counsel. Dead River is providing notice of this data security event to other state regulators. Dead River is offering each of the potentially affected individuals one year of triple-bureau credit monitoring and restoration services, at no cost to the individual.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact our privacy and data security legal counsel, Peter Guffin at 207-791-1199 or Clifford H. Ruprecht at 207-791-1186, of the law firm of Pierce Atwood.

Sincerely,

Leslie Anderson
Director of Risk and Corporate Counsel
Dead River Company

Exhibit A

Delivering on A promise.℠

Dead River Company

Dear _____:

I hope you've had time to read the letter I sent you last week, telling you about some malware (malicious software) that was placed on Dead River Company's computer systems without our permission. We understand that letter may have been unsettling.

As I said I would, I am writing to follow up to be sure that you understand this incident and the help we are providing you. I want to tell you three important things.

First, we're sorry. Let me offer our sincerest apologies for any inconvenience or frustration this episode may have caused you. We take this incident, and the security of your information, seriously. We value your business, but more importantly, we value your trust.

Second, we're eager to help. We understand that you may have additional questions or concerns. Please don't hesitate to call Dead River Company's Customer Relationship Center and ask for assistance if you feel you need it. We are also offering you one-year of identity and credit monitoring to provide you with protection and peace of mind in the wake of this incident. The enclosed communication provides detailed information about these services from a leading vendor, and instructions about how you can sign up for them, at no cost to you.

Finally, I want to provide you with some legally required notifications. Unfortunately, these kinds of cyber attacks targeting businesses, governments and individuals are common enough that states have laws requiring certain notifications in such events. The enclosed notice contains additional information in accordance with state requirements.

The enclosed information is important. Please take some time to read it carefully.

Again, we are sorry that this incident happened. We are eager to help. If you have any questions, or would like to discuss this further, please contact Dead River Company's Customer Relationship Center at 1-855-317-4837, Monday through Friday, 8:00 a.m. – 5:00 p.m.

Sincerely,

Robert A. Moore
President
Dead River Company

82 Running Hill Road • Suite 400 • South Portland, Maine 04106-3218
Phone: (207) 358-5800 • Fax: (207) 773-1302 • Toll Free: 1-800-287-5841 • www.deadriver.com

State Notification Requirements

About your personal information

On March 6, 2013, Dead River Company detected the presence of malware on its computer network. The Company immediately commenced an investigation into the incident, and retained third-party cyber forensic experts to assist in the identification, isolation and removal of the malware from its network, as well as the identification of what information on its network, if any, was at risk as a result of the malware. The affected network was shut down on March 8, effectively disabling the malware.

Although this investigation is ongoing, it appears that the personal information of a very small number of Dead River Company customers may be at risk as a result of this malware. These customers are individuals who, either over the phone or in person and on or between March 6, 2013 and March 8, 2013:

- Provided credit card or debit card information;
- Provided financial account information for an electronic funds transfer; or
- Applied for charge approval privileges

These transactions are those that required a Dead River Company customer service representative to type information into a web browser from a Company computer. The personal information at risk may include your name, address, Social Security Number, and financial account, debit or credit card number.

Dead River Company is providing this notification to all customers who may have provided financial information during this period of time, either over the phone or in person, to a Dead River Company customer service representative in order to render payment or apply for charge-approval privileges.

We are not aware of any actual or attempted misuse of your personal information. However, we want to provide you with advice on ways to protect yourself.

Enroll in Free credit monitoring service for 12 months

We have retained AllClear ID to provide – at no cost to you – one year of its AllClear Credit Monitoring, ID Theft Insurance Policy, and AllClear ID Repair Services under its AllClear Pro Plan. Enrollment instructions are included in this packet.

Recommendations to protect you from identity theft

To further assist in protecting against possible identity theft or other financial loss and in addition to activating your AllClear ID program membership, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. The contact information for these bureaus is below.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file, which alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay

your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

Instances of known or suspected identity theft should also be reported to law enforcement, and to your state's Attorney General. Your state Attorney General may also have advice on preventing identity theft.

AllClear ID
ALERT NETWORK

DON'T WAIT. SIGN-UP NOW FOR YOUR COMPLIMENTARY IDENTITY PROTECTION.

www.Enroll.AllClearID.com

AllClear ID provides advanced and effective identity theft protection to help safeguard your personal information. AllClear ID protection gives you the ability to respond to threats to your identity faster by delivering secure phone alerts that enables you to take immediate action if you suspect your identity is at risk.

Three Easy Ways to Enroll:

Have questions? Call {AllClearIDPhone}

Online: Visit enroll.allclearid.com

By Phone: Call 1-866-979-2595 Mon. – Sat., 8am–8pm Central Time

By Mail: Use form included in letter

Your Redemption Code: {ActivationCode}

Complete identity protection from AllClear ID includes:

- **Credit Monitoring:** Monitors credit activity and sends alerts when banks and creditors use your identity to open new accounts*
- **Fraud Detection:** Monitors thousands of sources for stolen and compromised data
- **Fast & Secure Alerts by Phone:** Delivers quick, secure, detailed alerts if your personal information is threatened, so you can take fast action to protect your identity
- **Live AllClear™ Investigators:** When you receive a secure phone alert and suspect fraud, press the star key to be connected to an investigator dedicated to your case
- **Identity Repair:** Award-winning AllClear Investigators work to fully restore your identity
- **$1,000,000 Identity Theft Insurance:** Covers certain financial losses related to recovering your identity
- **Lost Wallet Protection:** AllClear Investigators help cancel and replace credit and debit cards if your wallet is lost or stolen
- **Long-term Coverage:** Identity repair provided after the initial service period ends
- **ChildScan:** Detects & repairs identify theft for minors under 18 years old

*** Please Note: Additional action after registration may be required by you in order to activate certain features of the service. Mailed registrations may take up to ten (10) business days before the registration is received and you are able to log-in to activate these features.**

AllClear ID was awarded 5 Stevie Awards for outstanding customer service

AllClear ID is rated A+ by the Better Business Bureau

BBB. | A+

Exhibit B

Notice to Dead River Company Employees
March 18, 2013

As you know, on March 6th, Dead River Company discovered the presence of malware on some of our internal computers. We immediately began an investigation and retained the services of outside cyber forensic experts to help us identify, isolate, and eradicate the malware as well as prevent a recurrence.

Investigators worked to determine the scope and impact of the problem. This is an ongoing, careful, and deliberate process that has **now revealed the possibility that some personal information – from a limited number of employees – may have been compromised.**

This possibility exists ***only*** **if you used a company computer connected to a Dead River Company network between the dates of March 6, 2013 and March 8, 2013 and:**

- you typed information (i.e., user name and password) to access personal accounts such as bank or credit cards; or
- you typed in credit card numbers for personal or company business; or
- you typed in any personal identifying information using a web browser, such as your Date of Birth or Social Security Number.

If you think you may be affected, we recommend you:

- call 207-358-5800 and ask to speak to Guy Langevin, Vice President of Human Resources, so he can assist you with credit monitoring if you were affected;
- change all your personal online user names and passwords; and
- monitor your financial account statements for any unusual or suspicious activity.

Regarding March 7th paychecks, we want to reiterate that there was no danger of any improper access of information through direct deposit of paychecks. Direct deposit for the March 7th pay date was done on March 5th. The malware did not arrive until March 6th. Paper checks for the March 14th pay date were created out of caution while investigators worked to determine the scope and impact of the problem.

We understand that this malware attack has made it difficult for all of us to continue to serve our customers, but because of your efforts, we have continued to provide the service they have come to expect from Dead River Company. It's unfortunate that some of us are possibly facing personal impacts from the malware. With continued diligence we will put this episode behind us and move forward stronger than ever.

Exhibit C

Dead River Company

March 18, 2013

Dear Valued Customer,

On March 6, 2013, Dead River Company discovered the presence of malware on its network. We immediately began an investigation and retained the services of third-party cyber forensic experts to help us identify, isolate and eradicate the malware, as well as determine what information, if any, the malware compromised, and prevent a recurrence. This investigation is ongoing.

At this point in the investigation, we believe there are a very small number of customers whose information may be at risk as a result of the malware. These customers are individuals who, between March 6, 2013 and March 8, 2013:

- Provided a credit or debit card for payment over the phone or in person,
- Provided information for an electronic funds transfer for payment over the phone or in person, or
- Applied for charge approval privileges over the phone or in person.

These transactions are those that required a customer service representative to type information into a web browser from a company computer. At this time, we believe any such transactions occurring before March 6, 2013 and after March 8, 2013 were not affected by the malware.

You are receiving this letter because our records reveal that you provided information to a Dead River customer service representative, over the phone or in person, on or between March 6, 2013 and March 8, 2013, to perform any of the three transactions listed above. You will soon receive another written correspondence from us, which offers you one (1) free year of credit monitoring services. In the meantime, we encourage you to review your financial and credit card account statements for any unusual activity.

We want to take this moment to offer our sincerest apologies for any inconvenience or frustration this may have caused you. We take this incident, and the security of your information, seriously. We value your business, but more importantly, we value your trust.

If you have any questions, or would like to discuss this further, please contact Dead River Company's Customer Relationship Center at 1-855-317-4837, Monday through Friday, 8:00 a.m. – 5:00 p.m. Or, you may call Dead River Company's Privacy Line directly at 1-877-309-0195, Monday through Friday, 9:00 a.m. – 6:00 p.m.

Sincerely,

Robert A. Moore
President

82 Running Hill Road, Suite 400 • South Portland, Maine 04106
www.deadriver.com