Delivering on A promise.℠

Dead River Company

April 10, 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 Sorrell:

We are writing to supplement our notice to your office dated March 22, 2013. Dead River Company ("Dead River"), 82 Running Hill, Suite 400, South Portland, ME 04106, sent a letter to your office informing you of pertinent facts known at that time related to the March 6, 2013 detection of malware on Dead River's computer network. For your convenience, attached as **Exhibit A**, is a copy of the March 22, 2013 letter sent to your office with exhibits.

Dead River is contacting your office to notify you of ten (10) additional New Hampshire residents potentially affected by this data event bringing the total number of potentially affected New Hampshire residents to two hundred and ten (210). The additional ten (10) New Hampshire residents are individuals who paid Dead River using a credit card number on behalf of a business. On or about April 8, 2013, the individuals associated with the credit cards used by the Dead River business customers were sent written notice in substantially the same form as the sample notice attached to this letter as **Exhibit B**.

Dead River is providing you this update as the identity of these individuals had not yet been ascertained when Dead River first notified your office of this potential data event. The additional ten (10) New Hampshire residents were identified after Dead River confirmed with each of its small business customers that credit cards used to pay Dead River were or were not associated with individual persons.

Should you have any questions regarding this supplemental 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

Attachments

EXHIBIT A

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

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

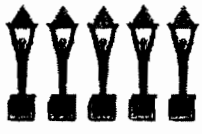
Your Redemption Code: {ActivationCode}

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

EXHIBIT B

[First_Name] [Last_Name] April 8, 2013
[Address_Line_1]
[Address_Line_2]
[City], [State] [Zip]

Dear [First_Name] [Last_Name],

Recently, 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. Because there is potential for you information to be at risk, we are offering you one-year of identity protection 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.

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.

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

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

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

www.Enroll.AllClearID.com

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

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 (866) 979-2595

Online:	Visit enroll.allclearid.com
By Phone:	Call (866) 979-2595 Mon. – Sat., 9am–9pm EST
By Mail:	Use form included in letter
Your Redemption Code:	{RedemptionCode}
Enrollment Deadline:	June 30, 2013

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 your phone alerts and monitoring options. 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+

AllClear ID

Register for AllClear ID Protection

ALLCLEAR ID CORPORATE ADDRESS
823 CONGRESS AVE, SUITE 300 –AUSTIN, TX 78701

ALLCLEAR ID MAIL PROCESSING CENTER
P.O. BOX 3356 – SUWANEE, GA 30024-9847

To register by mail, complete this form and mail to **AllClear ID** at the address above.
You do not need to complete this form if you register online at enroll.allclearid.com or by phone at (866) 979-2595.

INSTRUCTIONS:

- **Fill in your personal information.** All fields are required unless specified otherwise. Please provide at least one phone number.
- **To register additional family members**, please use a separate form. **To register a minor** under 18 years old, please provide information for the parent or legal guardian. Correspondence concerning a minor will be addressed to the parent or legal guardian.
- If you have an **AllClear ID** Redemption Code or Promotion Code, enter it at the top of the Registrant Personal Information Section.

Please **PRINT CLEARLY** in **BLACK INK** within the boxes.
Shade the bubbles completely. Correct: ● Incorrect: ⊘ ⊘

A B C D E 0 1 2 3 . _ –

ADDRESS INFORMATION

Please do not write in this section. Please use the "Change of Address" section to make corrections.

«FIRSTNAME» «MIDDLENAME» «LASTNAME» «SUFFIX»
«ADDRESS1»
«ADDRESS2»
«CITY», «STATE» «ZIPCODE»

REDEMPTION CODE: «REDEMPTIONCODE»

REGISTRANT PERSONAL INFORMATION

GENDER
O MALE
O FEMALE

DATE OF BIRTH (MM/DD/YYYY) / /

SOCIAL SECURITY NUMBER (Required) – –

MOBILE PHONE NUMBER – –

HOME PHONE NUMBER – –

WORK PHONE NUMBER – –

EMAIL ADDRESS (For Online Account Access)

PARENT/ LEGAL GUARDIAN INFORMATION (If Registering a Minor)

FIRST NAME

MIDDLE LAST NAME

SUFFIX

GENDER
O MALE
O FEMALE

DATE OF BIRTH (MM/DD/YYYY) / /

SOCIAL SECURITY NUMBER (Required) – –

MOBILE PHONE NUMBER – –

HOME PHONE NUMBER – –

WORK PHONE NUMBER – –

EMAIL ADDRESS (For Online Account Access)

CHANGE OF NAME OR ADDRESS (Optional)

FIRST NAME

MIDDLE LAST NAME

SUFFIX

RESIDENCE ADDRESS LINE 1

RESIDENCE ADDRESS LINE 2 (Optional)

CITY

STATE

ZIP

By registering for AllClear ID, I agree to the AllClear ID End User License Agreement (enclosed) and I authorize AllClear ID, who provides Identity Theft Protection, and its service providers to obtain and monitor my own credit information from credit reporting agencies and send this information to me alone for my own use. I certify that I am the parent/legal guardian of any children that I register for the AllClear ID service. *Please note that additional action after registration may be required by you in order to activate your phone alerts and monitoring options. 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.*

Under federal law, you have the right to receive a free copy of your credit report once every twelve months from each of the three national consumer reporting agencies. To request your free annual report under that law, visit www.annualcreditreport.com or call (877) 322-8228.

End User Services Agreement

This agreement ("Agreement") is made by & between **AllClear ID, Inc.**, formerly "Debix" ("**AllClear ID**"), having an address of 823 Congress Avenue, Ste. 300, Austin, TX 78701, & you ("you"). As of the date you register for or enroll in the Service, the parties agree as follows:

1. **Definitions.** The "Service" means the Premium Service and/or the Basic Service, for which you enroll, as the case may be, determined in accordance with your registration & the terms hereof. The "**Premium Service**" is one of the following, depending on your election at registration: (i) AllClear ID Pro (ii) AllClear ID Plus (iii) AllClear ID Guarantee. A Premium Service may include a Service that a third party is purchasing for you on your behalf, i.e. it may be free to you but still a Premium Service. The "**Basic Service**" is AllClear ID Basic and is provided at no cost. References to the Service include any use you make of the interface available at www.debix.com or www.allclearid.com (collectively, the "Site").

2. **Provision of the Service.** AllClear ID will provide you with the Service you elected at registration subject to the terms and conditions of this Agreement. A detailed description of the Service for which you are registered can be found in your profile which may be accessed by logging into the Site. **Term & Termination Re: Basic Service.** Your subscription to the Basic Service commences upon your registration, covers identity theft events *occurring* after registration, & terminates upon the earlier of (i) AllClear ID's notification to you of its discontinuance of the Basic Service offering, (ii) AllClear ID's election to terminate your Basic Service if you do not opt-in at the end of the then-current subscription period, or (iii) your election to terminate your subscription to the Basic Service, each of which may occur at any time.

3. **Subscription Fee.** The subscription fee for the Premium Service, if applicable, will be billed at the retail price currently in effect, at a previously approved & agreed-upon pricing, or in accordance with the applicable promotion code on the Site & according to the terms described herein. If you have questions regarding your fee, please contact customer service toll free at the applicable phone number listed above. AllClear ID will continue to bill your payment method on a periodic basis until the expiration or termination of your Premium Service. You may cancel your subscription for the Premium Service (if any) for which you have registered in accordance with Section 7. If you pay monthly & wish to cancel, you must call Customer Service prior to the start of the following month. If you pay for multiple months in advance & cancel your Premium Service prior to the end of the period for which you have paid, AllClear ID will refund payment for only any full, unused months. If someone has paid on your behalf and you cancel, you will not receive a refund.

4. **Free Trial.** If you receive a Premium Service as the result of a third party procuring it for you on your behalf, this Section is not applicable to you. If you are subscribing to a Premium Service on your own behalf, it may start with a free trial period. If you do not cancel before the end of such free trial period, you agree that AllClear ID is authorized to charge you a monthly subscription fee for such Premium Service at the current rate to the payment method you provided during registration. You must provide a valid payment method to enroll in any free trial. AllClear ID will begin billing your payment method for monthly subscription fees at the end of the free trial period, unless you cancel prior to the end of the free trial period. You will not receive a notice from us that your free trial period has ended or that the paying portion of your subscription has begun. **If you cancel prior to the end of your free trial period, there will be no charges to your payment method.**

5. **Scope of Coverage; Term & Termination of Premium Service.** If you are a subscriber to a Premium Service, your subscription to such Premium Service commences upon your registration. Additional action may be required by you after registration in order to activate your phone alerts and monitoring options. Failure to activate or use an available feature of the Service does not affect the cost of the Service. The Premium Service covers identity theft events discovered after registration. If a third party has procured the Premium Service on your behalf, your subscription to the Premium Service will terminate at the end of the term specified during registration, unless you opt to re-enroll. If you are subscribing to a Premium Service on your own behalf, then at the end of your initial subscription period, your subscription will automatically renew on a month to month basis until you terminate it in accordance with this Section or fail to provide payment when due. In addition, the Premium Service may be terminated or suspended at any time with or without notice if payment is not received when due or if you breach any of the terms & conditions set forth herein. If your subscription to the Premium Service expires because you fail to renew it or fail to provide payment when due, AllClear ID may convert you to the Basic Service for one (1) year, subject to the terms & conditions applicable to the Basic Service as set forth herein. If you transfer from one Service to another, the terms and description of such newly elected Service will apply. In the event that you elect to transfer to a new Service, you will forfeit any remaining entitlement in your previous Service. Notwithstanding the foregoing, if you are affected by two separate incidents from the same source company, your newly elected Service will continue after the term of your previous Service, with no forfeiture.

6. **Restrictions.** You will use any Service only for your benefit & for its intended purpose. You will not permit any third party to: (a) except as expressly set forth in this Agreement, use, copy, modify, create derivative works of, distribute, sell, sublicense, or transfer the Service; (b) remove or alter any AllClear ID notices or markings, or add any other notices or markings within the Service; (c) decrypt or attempt to decrypt the Service; (d) derive or attempt to derive the source code of or decompile the Service; or (e) disassemble or reverse engineer the Service. If statutory rights make any part of this section void, you will provide AllClear ID with detailed information regarding any such activity.

7. **Ownership.** This Agreement confers no ownership rights to you & is not a sale of rights in the Service. Ownership of all right, title, & interest in or to the Service & all Feedback & all intellectual property rights embodied therein are & will remain AllClear ID's exclusive property. You will take all reasonable actions to perfect such ownership, including without limitation executing instruments of assignment. AllClear ID reserves all rights in the Service & the intellectual property rights embodied therein not expressly granted hereby. The Service contains AllClear ID proprietary & confidential information. You will hold such information in confidence & not use or disclose it in any way except as expressly permitted hereunder, using no less than reasonable care. If you provide feedback &/or generate data in using the Service ("**Feedback**"), except to the extent set forth in our Privacy Policy you hereby assign all right, title, & interest therein to AllClear ID. If such assignment is ineffective, you agree to grant to AllClear ID a non-exclusive, perpetual, irrevocable, royalty free, worldwide license to use, reproduce, sublicense, distribute, modify, & otherwise exploit such Feedback without restriction.

8. **Support.** In connection with the Service, AllClear ID will provide the support specified on the Site from time to time.

9. **Disclaimer of Warranties.** ALL SERVICES ARE PROVIDED TO YOU "AS IS," WITHOUT WARRANTY, & ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PURPOSE, NON-INTERFERENCE, ACCURACY, & NON-INFRINGEMENT ARE DISCLAIMED. ALLCLEAR ID DOES NOT WARRANT THAT THE SERVICE WILL OPERATE WITHOUT INTERRUPTION, BE ERROR-FREE, OR ACHIEVE SPECIFIC RESULTS. THE SERVICE IS NOT A CREDIT COUNSELING SERVICE. ALLCLEAR ID DOES NOT PROMISE TO HELP YOU IMPROVE YOUR CREDIT RECORD, HISTORY, OR RATING.

10. **Authorization.** You authorize AllClear ID & its service providers to obtain & monitor your own information from credit reporting agencies and/or other monitoring services & send this information to you for your own use. You agree that this authorization shall constitute written instructions to obtain your credit information in accordance with the Fair Credit Reporting Act. If AllClear ID is unable to process the credit monitoring request, AllClear ID will make a reasonable effort to contact you. You certify that you have the express consent of all adults that you register to submit their information to AllClear ID with the intent to utilize the Service & to agree to this Agreement on their behalf. You also certify that each adult that you register for the Service has read & accepted the terms & conditions of this Agreement, and authorizes AllClear ID, & its service providers, to obtain & monitor his or her own credit information from credit reporting agencies & send this information to him or her alone for his or her own use. You agree that this authorization shall constitute written instructions to obtain his or her credit information in accordance with the Fair Credit Reporting Act. You certify that you are the parent/legal guardian of any and all children that you register for the Service. Information that AllClear ID collects from you will be treated in accordance with the AllClear ID Privacy Policy: https://www.allclearid.com/legal/privacy-policy.

11. **Limitation of Liability.** ALLCLEAR ID WILL NOT BE LIABLE FOR INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES (INCLUDING WITHOUT LIMITATION COST OF COVER), EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ALLCLEAR ID SHALL NOT BE LIABLE FOR ANY 3RD PARTY CLAIMS. OUR CUMULATIVE LIABILITY WILL BE LIMITED TO WHAT WAS PAID BY YOU OR ON YOUR BEHALF FOR THE SERVICE IN THE 12 MONTHS BEFORE THE CLAIM. THIS SECTION IS A FUNDAMENTAL PART OF THE BASIS OF OUR BARGAIN, WITHOUT WHICH ALLCLEAR ID WOULD NOT BE ABLE TO PROVIDE THE SERVICE, & WILL APPLY DESPITE THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. If some or all of the limitations & exclusions in Sections 11 & 13 are held unenforceable, warranties will be disclaimed, & AllClear ID's liability will be limited to the greatest extent permitted under applicable law.

12. **Compliance with Law.** You warrant that in using the Service, you will comply with all applicable laws, including without limitation with all regulations of agencies of the U.S. Government regarding export & re-export restrictions. You will hold harmless & defend, at our option, AllClear ID from any third party claim against AllClear ID arising from your failure to comply with this Agreement.

13. **Termination Procedure.** AllClear ID may require reasonable identification verification before completing any request to terminate the Agreement or to cancel the Service.

14. **General. Any notice hereunder will be in writing & sent by mail, return receipt requested, by e-mail, or by reputable courier addressed to the other party (i) if to AllClear ID, the address set forth above or at support@allclearid.com & (ii) if to you, at the address or e-mail address you provide when you register for the Service, or at such other address of which you give notice in accordance with this provision. It is your responsibility to keep your contact information up to date. Notice will be deemed to have been given when delivered (as confirmed by receipt or other confirmation) or, if delivery is not accomplished by fault of the addressee, when tendered. This Agreement will be governed by the laws of Texas, without regard to conflict of laws. The U.N. Convention on Contracts for the International Sale of Goods does not apply. All disputes will be brought only in a court located in Travis County, TX, & to the fullest extent permitted under applicable law, you consent to the same as the exclusive jurisdiction for claims arising hereunder & waive any objection to venue of such courts. If any provision hereof is held unenforceable, the remaining provisions will be unaffected. Your rights may not be assigned without written consent by AllClear ID. AllClear ID may assign this Agreement. Failure or delay in enforcing this Agreement will not be deemed a waiver. This Agreement constitutes the entire agreement between the parties & supersedes all prior or contemporaneous agreements with respect to its subject matter. This Agreement may not be amended except in writing or a subsequent click to accept or telephonic method offered by AllClear ID. Certain businesses not affiliated with AllClear ID may display the AllClear ID or AllClear Guarantee logo and offer access to the AllClear ID service. Such use or offers should not be construed, in any respect, as an endorsement or guarantee by AllClear ID of the security practices of such businesses.** Upon any termination or expiration of this Agreement, all terms will cease, except Sections 5 - 14, which survive.