



February 18, 2014

Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

On January 17, 2014, Kenerson Associates, Inc. ("Kenerson") was notified by BenefitMall, its payroll processing company, that BenefitMall had recently learned that an unknown person or persons gained unauthorized access to a BenefitMall computer system in November 2013. BenefitMall further advised Kenerson that upon learning of the incident, it limited access to the computer system in question, conducted an investigation, and hired a computer forensics firm to determine what information may have been accessed. Based on the forensic review, BenefitMall determined that personal information pertaining to eighteen (18) of Kenerson's current and former employees was potentially accessed, including name, address and social security number.

While BenefitMall indicated that there was no evidence that anyone used Kenerson's employees' personal information, it advised Kenerson that it may be required to alert its employees of the incident. Additionally, BenefitMall established an incident inquiry hotline that Kenerson's employees could use for general inquiries and to activate one year of free credit monitoring services. BenefitMall also provided a list of the Kenerson employees impacted by the incident and a draft letter that Kenerson could use to notify its employees of the incident.

On that same day, January 17, 2014, Kenerson sent a letter to the one (1) New Hampshire resident impacted by the incident. The letter advised this individual of the incident and recommended certain precautionary safeguards, including calling the BenefitMall incident inquiry hotline with general inquiries and to obtain free credit monitoring; placing a fraud alert on credit files and instructions on how to do so; and obtaining free credit reports. The letter is attached for your review. As an additional precaution, Kenerson also opened new bank accounts for its direct deposit program because BenefitMall is Kenerson's payroll processing company.

Please rest assured that Kenerson takes its employees' privacy very seriously, and it will continue to work diligently to protect their personal information. Further, BenefitMall has assured us that safeguarding the information that Kenerson entrusts to them is their utmost priority. Should you have further questions or concerns regarding this incident, please contact Bill Walsh at Kenerson Associates, Inc., 50 Dunham Road G200, Beverly, MA 01915 or by telephone at (978) 986-3110.

Regards,

Kenerson Associates, Inc.

Enclosure



January 16, 2014

Michelle Ricci
Kenerson Associates Inc
50 Dunham Road G200
Beverly, MA 01915

Dear Michelle Ricci:

At BenefitMall, we pride ourselves on helping small businesses with their important payroll and HR administrative functions. In carrying out our duties, we take data security very seriously. We recently learned that an unknown person or persons in November 2013 gained unauthorized access to a BenefitMall computer system. Upon learning of the incident, we limited access to the computer system in question, conducted an investigation, and hired a respected computer forensics firm to determine what information may have been accessed. Based on this review, we believe that personal information pertaining to certain of your current and/or former employees was potentially accessed.

We have no evidence that anyone has used your employees' personal information, but we want to bring this incident to your attention because you may be legally required to alert your employees or to take other steps as required by law. To assist you in managing this matter, we have:

- Made arrangements to facilitate your communications with these employees, to provide identity monitoring services to them, and to establish a toll-free number for their inquiries at no cost to you or them. You may access these services for the employees by calling the BenefitMall Incident Inquiry Line at (877) 282-6407 Monday – Friday between the hours of 9:00 AM EST – 5:00 PM EST within 30 days of the date of this letter to obtain the toll-free number that the employees can use for general inquiries and to enroll in identity monitoring services. That toll-free number for the employees will be available for a period of 60 days after you call the BenefitMall Incident Inquiry Line to activate these services. Please note that you will not be provided legal advice and that you should independently determine any legal obligations that you might have.
- Attached a list of the current or former employees whose personal information may have been accessed and who qualify for the services referenced above, along with an identification of the type of personal information that may have been accessed [Attachment A].
- Provided a sample draft letter that you may use to inform those employees and former employees of the incident, along with practical suggestions that you may send to those employees and former employees on steps that they can take to protect themselves [Attachment B].

BenefitMall places great importance on privacy and security. We sincerely apologize for any inconvenience or concern that this incident may cause you. Questions regarding the matter may be directed to Keith Terreri at (469) 791-2155.

Sincerely,

A handwritten signature in black ink, appearing to read "S. Kirksey", is written over a light gray rectangular background.

Scott Kirksey
Vice President, Chief Financial Officer
BenefitMall

Enclosure: [Attachment A, Attachment B]

Attachment B
Sample Draft Letter for BenefitMall Clients to Current and Former Employees

Please note: This sample draft letter is provided as a helpful tool and starting point for your use in notifying your employees. It is not intended to satisfy any legal obligations that might pertain to you and should not be construed as legal advice.

Dear [Former] Employee:

We recently learned that an unknown person or persons gained unauthorized access in or around November 2013 to a computer system belonging to our payroll processor. Upon learning of the incident, the payroll processor immediately limited access to the computer system in question and conducted an investigation to determine what information may have been accessed.

Unfortunately, the payroll processor's review determined that some of your personally identifiable information may have been accessed without authorization, including your **[insert the information about this employee that may have been accessed from Attachment A]**.

While there is no evidence that anyone has used your personal information, the payroll processor has arranged for free identity monitoring at no cost to you and has established a toll-free number for your inquiries. The identity monitoring product is known as First Watch ID. Please call **[insert the toll-free number for your employees' use that you received when you called the BenefitMall Incident Inquiry Line]** Monday through Friday between the hours of 9 a.m. and 7 p.m. ET for general inquiries and to enroll in First Watch ID. After enrollment, you will receive one year of identity monitoring from time of activation.

Please note that this toll-free number for employee inquiries and enrollment in First Watch ID will be available for a period of 60 days from **[insert the date that you called the BenefitMall Incident Inquiry Line to access these services for your employees]**. The activation code that you need to enroll in First Watch ID is **[insert the activation code for this employee that you received from the BenefitMall Incident Inquiry Line]** and must be provided by you when you call the toll-free number to enroll.

You will also find attached to this letter some steps that you can take to protect your identity.

Our payroll processor has apologized for the inconvenience and concern that this causes. They have assured us that safeguarding the information that we entrust to them is their utmost priority. I also extend my apologies for this inconvenience.

Please let me know if you have questions.

Sincerely,

Steps You Can Take to Protect Yourself

For your additional protection, you can contact the fraud department at any one of the three credit reporting agencies to inform the credit reporting agencies that you may be the victim of identity theft and to request that a “fraud alert” be placed on your files. A fraud alert is a consumer statement added to your credit file that warns creditors about possible fraudulent activity within your accounts and requests that any creditors contact you before opening a new account or changing existing accounts. There is no charge for this service, and it is easy to request. You can call any one of the three major credit reporting agencies listed below. As soon as you alert one credit reporting agency, it will notify the other two to place fraud alerts on your accounts as well.

<u>Credit Agency</u>	<u>Fraud Alert Toll-Free No.</u>	<u>Website</u>
Equifax	1-888-766-0008	www.equifax.com
Experian	1-888-397-3742	www.experian.com
TransUnion	1-800-680-7289	www.transunion.com

There are a number of other ways that you can protect yourself from fraud and identity theft:

- You are entitled under U.S. law to one free credit report annually from each of the three major credit reporting agencies listed above. Reviewing your credit reports will allow you to confirm that no new accounts have been opened without your knowledge and may give you early notice of any potential fraud or incidents of identity theft. To order a free credit report, you can visit www.annualcreditreport.com or call toll-free (877) 322-8228.
- When you receive your credit reports, you should review them carefully. If you notice suspicious activity on the report, you should call your local police or sheriff’s offices and file a police report of identity theft. You should obtain a copy of the police report because you may need to provide the report to creditors to clear your records. You should also file a complaint with the Federal Trade Commission, who may be contacted at 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/idtheft, or 1-877-ID-THEFT (1-877-438-4338). Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. You should also file a complaint with the Attorney General’s office in your state of residence.
- Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you continue to check your credit reports periodically. Identity thieves sometimes hold on to personal information for a period of time before using it. Checking your credit reports periodically can help you spot potential problems and address them quickly. For additional information, you may wish to visit the FTC’s web site at www.ftc.gov/idtheft.
- You may also obtain additional information about fraud alerts, security freezes, and steps to avoid identity theft from the Attorney General’s office in your state of residence. That office may offer further information and support to help you guard against fraud and identity theft.



Date: 01-17-2014

To: Kenerson Associates – Michelle Ricci

Re: Identity Monitoring and Toll-Free Number for General Employee Inquiries

Dear BenefitMall Customer:

BenefitMall has made arrangements with Intelligent Business Concepts Inc. (IBC) to: (1) provide an identity monitoring product to certain of your current and former employees that were identified by BenefitMall in a prior letter to you, and (2) establish a toll-free number for their general inquiries at no cost to you or them.

This identity monitoring product is known as First Watch ID. Please have these employees call 877-280-7184 Monday through Friday between the hours of 9 a.m. and 7 p.m. ET for general inquiries and to enroll in First Watch ID. After enrollment, these employees will receive one year of identity monitoring from time of activation.

Please note that the toll-free number for employee inquiries and enrollment in First Watch ID will be available for a period of 60 days from the date that you called the BenefitMall Incident Inquiry Line. The activation codes needed for these employees to enroll in First Watch ID will be sent to you via secure email and must be provided by you to these employees BEFORE they can call the toll-free number to enroll.

Additionally, you will find:

1 – An overview of the First Watch ID product that can be distributed to your current and former employees that were identified by BenefitMall in a prior letter to you.

2 – Approved language for use in your Notification letter to your employees.

BenefitMall sincerely apologizes for any inconvenience or concern that this incident may cause you.

SOIPLER SO VN
DEPT OF MCH
STATE OF NH