Melanie Flowers
Privacy Officer
700 Tower Drive, Ste. 300
Troy, MI 48098
(248) 813-9800 x 3084
Melanie.Flowers@benesys.com

August 6, 2020

Attorney General Gordon MacDonald
New Hampshire Office of the Attorney General
Attn: Security Incident Notification
33 Capitol Street
Concord, NH 03301

Sent Via. Email to attorneygeneral@doj.nh.gov

Re: Notice of Security Event
N.H. Rev. Stat. § 359 – C:20

Dear Attorney General MacDonald:

I am writing on behalf of BeneSys, Inc., a Michigan company, to inform you of a security event pursuant to N.H. Rev. Stat. § 359 – C:20.

BeneSys is the third-party administrator for employee benefit plans, including health benefit plans. On July 22, 2020, a file containing the personal information of multiple plan participants in a client's plan was accidentally sent to a participant through our encrypted secure email system. The error was discovered on July 27, 2020, when the participant first opened the file with the personal information and immediately alerted us to the error. The file included participants' first and last names, Social Security numbers and bank account and routing numbers. One resident of New Hampshire was included in the disclosure.

We obtained a declaration from the recipient confirming that the file was permanently deleted and not further disseminated. Because the Trust is a covered entity under the Health Insurance Privacy and Protection Act ("HIPAA") the event will be reported to the Department of Health and Human Services. We informed the client of the event on July 28, 2020 and all affected participants were sent a letter on July 31, 2020 explaining the event and steps they could take to protect their personal information. The letter also contained an offer of 24 months of no-cost

credit monitoring service from Experian. We are implementing additional training to reduce the risk of similar errors in the future.

Please contact me with any questions about this letter.

Very truly yours,

Melanie Flowers

Melanie Flowers
Privacy Officer

t 248-813-9800 | f 248-813-9898 | www.benesys.com
700 Tower Drive, Suite 300 | Troy, MI 48098-2835

<<date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal-code>>

Notice of Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

On behalf of BeneSys Administrators, the third-party administrator for the [redacted], I am writing to you because a recent incident occurred in which BeneSys inadvertently disclosed your personal information to another participant in the Trust. This letter explains what happened, and what was disclosed.

What Happened

On July 22, 2020, a file containing your personal information and the personal information of other Trust participants was accidentally sent to a Trust participant through our encrypted secure email system (which requires a password and login to view e-mail messages). The error was discovered on July 27, 2020, when the participant opened the file with the personal information. The participant informed us that day that the email from BeneSys included a file with other participants' personal information. The participant reported that the file with your personal information was deleted and that the file has not been copied, forwarded or otherwise shared. The error was the result of our Eligibility department's failure to follow correct departmental procedures sending email.

What Information Was Involved

The file attached to the e-mail contained the Trust's Direct Deposit report, which included **your first and last name, your Social Security number, your bank account number and your bank's routing number,** as well as direct deposit reference number, transaction date, and payment amount information.

What You Can Do

Although the risk is low, because of the extent of the information disclosed, **you should immediately notify your bank that your account information has been disclosed.** In addition, we recommend that you closely monitor your bank and credit card accounts to ensure that no fraud occurs. We are offering you credit monitoring services through Experian for two years at no cost to you. **Please contact our privacy team at (888) 879-7834 or corporate.compliance@benesys.com if you are interested in credit monitoring or if you have any questions.**

What We Are Doing

Our IT department was able to retrieve and permanently delete the message and the file with your personal information from our secure email server so that the recipient cannot access it again. We have confirmed with the recipient that the file with your personal information was deleted and that the file has not been copied, forwarded or otherwise shared. Since discovering the error, we have addressed the employee involved who sent the file and have taken steps to reduce the risk of similar incidents. We sincerely apologize for this error and understand the concern it may cause you. Given the report and level of cooperation by the participant who received the file in error, we have no reason to believe that your information was further disclosed or compromised.

The privacy and protection of the information to which we are entrusted is a top priority of BeneSys and the Trust. Should you have any questions or require more information, please contact us at (888) 879-7834 or corporate.compliance@benesys.com.

Sincerely,

Melanie Flowers

Melanie Flowers
BeneSys Privacy Officer

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

   - Add a fraud alert statement to your credit file at all three-national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This alert will remain on your credit file for 90 days. A fraud alert alerts creditor of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name.
   - Add a security freeze to your credit file. A security freeze prevents your credit account from being shared with potential creditors, which can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies. Credit reporting agencies charge a $5 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of a police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include (documentation for both the spouse and the victim must be submitted when requesting for the spouse's credit report) (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Obtain a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com

2. Review all bills and credit card statements closely to determine whether you have been charged for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not

find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes delay their use of stolen personal information.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You can also obtain information from the FTC about fraud alerts and security freezes. You may contact the FTC by visiting www.ftc.gov or www.consumer.gov/idtheft, calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that you are the victim of identity theft, you should contact local police. You can also report such activity to the Fraud Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580. You may also obtain information about fraud alerts and security freezes from your state Attorney General and the credit reporting agencies.

4. We also recommend you closely monitor your financial accounts and access resources concerning identity theft, such as information the Internal Revenue Services has published at: http://www.irs.gov/Individuals/Identity-Protection and https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. As discussed in the Taxpayer Guide to Identity Theft, IRS Form 14039 can be filed with the IRS to report potential identity theft concerning your federal taxes. You also may want to check with the state(s) in which you file.

BeneSys

t 248-813-9800 | f 248-813-9898 | www.benesys.com
700 Tower Drive, Suite 300 | Troy, MI 48098-2835

<<date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal-code>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

To help protect your identity, BeneSys has retained Experian to provide two (2) years of complimentary identity theft protection. This product provides you with superior identity protection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **<<<date>>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bplus
- Provide your **activation code**: **<<<code>>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **<<<date>>>.** Be prepared to provide engagement number **<<<code>>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.

- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

The privacy and protection of the information to which we are entrusted is our highest priority. We apologize for any inconvenience this incident may cause you and thank you for your understanding and cooperation.

Sincerely,

Melanie Flowers

Melanie Flowers
HIPAA Privacy Officer
BeneSys, Inc.
(888) 879-7834
Corporate.compliance@benesys.com
www.benesys.com