BAIRD HOLM LLP
ATTORNEYS AT LAW
EST. 1873

Robert L. Kardell

1700 Farnam Street
Suite 1500
Omaha, NE 68102-2068
Tel: 402.344.0500
Fax: 402.344.0588
Direct: 402.636.8313
bkardell@bairdholm.com
www.bairdholm.com

September 3, 2021

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident
Client-Matter No.: Diversified Financial Services, LLC

To Whom It May Concern:

We are providing notification under N.H. Rev. Stat. § 359-C:19 (the "Act") of a breach concerning Personally Identifiable Information ("PII").

On August 4, 2021, Diversified Financial Services, LLC ("DFS") located in Omaha, Nebraska, discovered a data breach compromised the email account of one of its users. DFS conducted an investigation and engaged a cyber-forensics firm to determine the size and scope of the attack. The investigation determined that the date of the attack occurred from March 19, 2021 through June 14, 2021. DFS has conducted a manual review of documents in the email account to determine if the account contained PII. During the manual review we determined that the PII of 2 New Hampshire residents had been affected. Attached is copy of the notification which was sent to the residents of New Hampshire.

Sincerely,

Robert L. Kardell
FOR THE FIRM

BLK/BLK
Enclosure
DOCS/2682195.1

Diversified Financial
Relationship Driven.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Diversified Financial Services, LLC ("DFS") values our relationships with our customers and the community. We take seriously the obligation to safeguard our customers' sensitive personal information. Unfortunately, DFS recently experienced a cybersecurity incident that impacts some of our customers' personally identifiable information ("PII"). The purpose of this letter is to tell you what happened, what information was involved, what we are doing in response to this incident, and steps you can take to protect yourself against the possible misuse of your PII.

What Happened
On August 4, 2021 we discovered a cybersecurity incident that compromised a user's account in our business e-mail system. We hired an outside forensic computer expert to determine the size and scope of the attack. Our investigation determined that one or more unauthorized individuals from outside of our organization had access to one employee's e-mail account between approximately March 19, 2021 and June 14, 2021. The attack was the result of a phishing attack. The attack did not impact our business or other business systems. The only unauthorized access to PII may have occurred through the compromised e-mail account where the information was in the body of an e-mail or in an attachment (such as a spreadsheet used for internal business purposes).

What Information Was Involved
DFS manually reviewed the contents of the compromised e-mail account to determine if the account contained PII. Our investigation indicated that some of your information was contained in the compromised e-mail account. Information that may have been accessed includes full name and demographic information (such as address, city, state, and zip), and <<Data Elements>>.

What We Are Doing
After learning of the attack, DFS took a number of important steps to prevent similar incidents from occurring in the future. This included temporarily disabling the user's account while a password reset was performed, as well as, strengthening the technical procedures to access the account. DFS is also working to deploy additional technologies designed to prevent similar attacks including disabling old or unused access protocols, updating monitoring software, establishing new alert protocols, and providing expanded training for employees.

What You Can Do
To help detect and protect against possible misuse of your personal information, we recommend taking precautionary measures described below.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for <<CM Length>> months provided by TransUnion, one of the three nationwide credit reporting companies. Please see the handout at the end of this letter for enrollment instructions.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Review all personal account statements for possible indications of fraud and report all suspected transactions immediately to law enforcement.

More Information
Also included with this letter is information about other precautionary measures, including obtaining free credit reports and placing a fraud alert and/or security freeze on credit files.We understand that you may have questions about this incident that are not addressed in this letter. We have established a confidential, toll-free hotline with Epiq, a third party call center that is staffed with professionals familiar with this incident who can assist you with questions and steps you can take to protect yourself against identity theft and fraud. The hotline is available at 1-800-717-2379 Monday through Friday, from 8 am – 8 pm Central Standard Time.

We take the privacy and security of our customers' information seriously and apologize for any inconvenience or concerns because of this incident.

Sincerely,

Jeff E. Focht
President

TransUnion

Activation Code:
<<Activation Code>>

Complimentary <<CM Length>> Month *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery.

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR <<CM Length>> Month COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and credit score.

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

ADDITIONAL PRIVACY SAFEGUARDS INFORMATION

For Iowa Residents:
Residents of Iowa may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft with the following contact information:

Iowa Attorney General's Office
Director of Consumer Protection Division
1305 E. Walnut Street, Des Moines, IA 50319
1-515-281-5926
www.iowaattorneygeneral.gov

For Maryland Residents:
Residents of Maryland can contact the State of Maryland Attorney General's Office for more information about steps an individual can take to avoid identity theft using the following contact information:

Toll Free: 1-888-743-0023
Phone: (410) 576-6491
Fax: (410) 576-6566
E-mail: idtheft@oag.state.md.us
Mail: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202
ID Theft Web Site: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

For Massachusetts Residents:
Residents of Massachusetts have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York Residents:
Residents of New York may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office using the following contact information:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
www.ag.ny.gov

For North Carolina Residents:
Residents of North Carolina can contact the State of North Carolina Attorney General's Office for more information about steps an individual can take to avoid identity theft using the following contact information:

Toll Free: 1-877-5-NO-SCAM (1-877-566-7226)
Phone: (919) 716-6000
Mail: 9001 Mail Service Center, Raleigh, NC 27699-9001
Online Contact Form: https://ncdoj.gov/contact-doj/
ID Theft Web Site: https://ncdoj.gov/protecting-consumers/protecting-your-identity/

For New Mexico Residents:
Under the Fair Credit Reporting Act you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

For Oregon Residents:
Oregon Residents should report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392
www.doj.state.or.us

Fraud Alert Information
Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.equifax.com	www.transunion.com/fraud	www.experian.com
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information
Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report or notify your state's Attorney General Office. Attorney General Office contact information for each and every state and U.S. Territory can be found at https://www.naag.org/find-my-ag/. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the **Federal Trade Commission (FTC) at www.identitytheft.gov or at 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. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "Identity Theft - A Recovery Plan".

Security Freeze Information
You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze	TransUnion Security Freeze	Experian Security Freeze
PO Box 105788	PO Box 2000	PO Box 9554
Atlanta, GA 30348	Chester, PA 19016	Allen, TX 75013
https://www.freeze.equifax.com	http://transunion.com/freeze	http://experian.com/freeze
1-800-685-1111	1-888-909-8872	1-888-397-3742

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.) Your Social Security Number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.