CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

CAROLYN PURWIN RYAN
cpurwin@c-wlaw.com

JASON R. MCLEAN
jrmclean@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

May 13, 2019

Attorney General of the State of New Hampshire
State House Annex
33 Capitol Street
Concord, NH 03301

RE: Security Breach Notification

To Whom It May Concern:

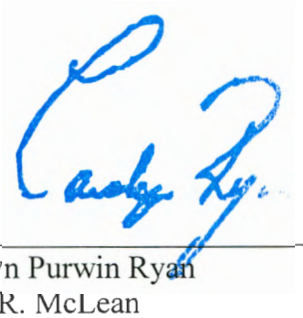
I serve as counsel for Akin Doherty Klein & Feuge, P.C. ("ADKF"), and provide this notification to you of a recent data security incident suffered by ADKF. On February 8, 2019 and February 14, 2019, Akin Doherty Klein & Feuge, P.C. ("ADKF") identified suspicious email activity consisting of an attachment seeking log in credentials and bounce back emails to one employee account that were not related to any emails sent by that employee. ADKF immediately undertook investigation, which included retaining forensic IT companies to analyze the affected accounts. It was ultimately determined that one account was potentially compromised, which may have allowed access to 4,007 individuals' personal information, 1 of which resides in New Hampshire. This information includes driver's license, financial information and/or Social Security number.

ADKF will be promptly notifying the affected individuals on May 14, 2019 and has provided them with complimentary credit monitoring for one year. A copy of the formatted letter is attached. As the letter indicates, ADKF will be offering credit monitoring and identity restoration services at ADKF's expense. ADKF is taking steps to comply with all applicable notification obligations.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: 

Carolyn Purwin Ryan
Jason R. McLean

ADKF Member of the AICPA and TXCPA

AKIN DOHERTY KLEIN & FEUGE, P.C.

Registered with Public Company Accounting Oversight Board

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>>

RE: Important Security Notification. Please read this entire letter.

Dear Sir or Madam:

We are writing to provide you notice of a recent security incident. On February 8, 2019 and February 14, 2019, Akin Doherty Klein & Feuge, P.C. ("ADKF") identified suspicious email activity related to one employee's email. ADKF immediately undertook an investigation, which included retaining an expert forensic company to analyze the affected accounts. It was ultimately determined that one account was potentially compromised, which may have allowed access to your personal information. This information includes driver's license, financial information and/or Social Security number.

At this time, ADKF has no information to suggest that any of this information was actually taken or has been used by any criminal actors. Nonetheless, out of an abundance of caution, we are providing you this notice. We take great care in the security of our technology systems, and regret that this incident has occurred.

What Did We Do to Protect Your Information?

Please be assured that ADKF has taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us. ADKF worked with data privacy experts and other professionals to further protect your privacy. We are concerned about both our valued customers and work force. We have already taken steps to fix the issue and strengthen our systems, and will continue to do so throughout this response process and beyond. We have also implemented the following protective measures:

- Implementing additional technological security measures; and
- Updating our password protocols.

Complimentary One-Year *my*TrueIdentity 3B Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*my*TrueIdentity) for one year 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, three-bureau 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 six-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 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,® Experian,® and Equifax,® 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.)

What You Can Do to Protect Your Information

Please remain vigilant by reviewing account statements and monitoring free credit reports. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to the enclosed list of additional actions to reduce your chance of identity theft below. As we go through this process I would ask the following:

1. Please let us know if you learn of or experience any suspicious activity with your credit cards, bank accounts or tax return processing. If you suspect identity fraud, you should report it to a law enforcement agency as you may be able to file a police report. We will cooperate with any investigations that state and federal law enforcement open and provide any information we can to assist their efforts.
2. Trust that we are doing, and will continue to do, everything possible to protect your personal information and reduce the likelihood of any further problems.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 855-424-7678 between 8:00 a.m. and 8:00 p.m. Central Time, Monday through Friday.

Sincerely,

Akin, Doherty, Klein & Feuge

Akin Doherty Klein & Feuge, P.C.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax, Consumer Fraud Division
P.O. Box 105069, Atlanta, GA 30348 Phone: 1.800.525.6285
www.equifax.com

Experian, National Consumer Assistance
P.O. Box 1017, Allen, TX 75013 Phone: 1.888.397.3742
www.experian.com

TransUnion Fraud Victim Assistance Department
P.O. Box 6790, Fullerton, CA 92834 Phone: 1.800.680.7289
www.transunion.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

➢ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➢ BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

➢ OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. To reach the FTC by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- Individuals can obtain information about steps to avoid identity theft from any of the above credit reporting agencies or their state Attorney General.