

RECEIVED

FEB 11 2019

CONSUMER PROTECTION

February 8, 2019

Gregory J. Bautista
914.872.7839 (direct)
Gregory.Bautista@wilsonelser.com

Sent Via Regular Mail

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent Katz, Sapper & Miller ("KSM") with respect to an incident involving the potential exposure of certain personal information described in detail below.

1. Nature of the possible security breach or unauthorized use or access

On January 5, 2019, KSM discovered that individuals' personal information may have been obtained by an unknown, unauthorized third party as the result of a security issue related to its use of Citrix ShareFile, a third-party file sharing service. After identifying unusual activity within a matter of hours, KSM took immediate action to remediate this third-party system, enhance security protocols and confirm that the issue could not lead to further unauthorized access. KSM also conducted an internal investigation, which determined that an unknown, unauthorized third party could have gained access to some individuals' personal information stored by KSM within its Citrix ShareFile environment, including the name, address and Social Security number of affected individuals. In very few instances, other data such as passport numbers, driver's license numbers and health insurance information may have been accessed if it was uploaded to ShareFile.

2. Number of New Hampshire residents potentially affected

Approximately twenty-one (21) New Hampshire residents were affected in this potential incident. KSM sent the potentially impacted individuals a letter notifying them of this incident on February 8, 2019. A copy of the notification sent to the potentially impacted individuals is included with this letter, which informs these New Hampshire residents about the 12 months of credit monitoring and identity theft protection services that is being offered to them.

1133 Westchester Avenue • White Plains, NY 10604 • p 914.323.7000 • f 914.323.7001

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Los Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix
San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

3. Steps KSM has taken relating to the potential incident

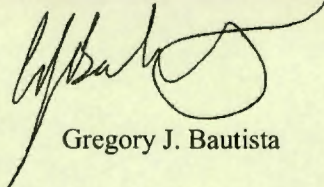
Upon learning of this issue, KSM immediately conducted an internal investigation to determine whether information in Citrix ShareFile was at risk and took steps to identify anyone potentially impacted by this incident. KSM has also taken steps to prevent a similar event from occurring in the future, including ensuring all clients reset their passwords as required by Citrix Sharefile of all users, including KSM clients.

4. Other notification and contact information

If you have any additional questions, please contact me at Gregory.Bautista@wilsonelser.com or (914) 872-7839.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Gregory J. Bautista



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>>

February 8, 2019

Dear <<Name 1>>:

We are writing to inform you of a security issue that potentially impacts your personal information. Katz, Sapper & Miller (KSM) recently identified a security issue related to our use of Citrix ShareFile, a third-party file sharing service. Our information technology team discovered the unusual activity within a matter of hours. We took immediate steps to remediate our third-party system, enhance security protocols and confirm that the issue could not lead to any further unauthorized access. We also conducted an internal investigation, which on January 5, 2019, determined that an unknown, unauthorized third party could have gained access to your <<Variable Data>> stored by KSM within our Citrix ShareFile environment. We have no confirmed evidence that any information was in fact compromised. However, out of an abundance of caution, we are taking steps to mitigate concerns and we are notifying you of this activity.

While we are confident that we have taken appropriate actions to secure our Citrix ShareFile environment, we understand the sensitivities surrounding this issue. While this potentially affected a small percentage of our clients, we sincerely regret any concern this may cause. Keeping in line with our values of trust and transparency, we felt it was necessary to inform you as soon as we had accurate information about what transpired.

Steps taken to enhance data security:

Third-party service provider Citrix has implemented a mandatory password reset for all users to mitigate any potential security issues. As a result, Citrix ShareFile users, including KSM clients, are required to update their ShareFile passwords within the platform. Our commitment to maintaining the confidentiality of the information entrusted to us remains paramount and resolute.

Services we are providing for you:

Because we value the security of your information, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for 12 months. This service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies.

To enroll, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the "Enter Activation Code" field, enter the following 12-letter Activation Code <<Activation Code>>. Follow the three steps to receive your credit monitoring service online within minutes.

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child.

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 following 6-digit telephone pass code <<Engagement Number>>, 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.

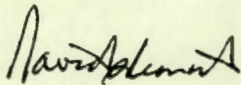
You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, 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.

Once you are enrolled, you will be able to obtain 12 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, change 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. You will receive help to restore your identity and up to \$1,000,000 in identity theft insurance with no deductible (policy limitations and exclusions may apply).

We understand that this situation may cause concern and frustration. We sincerely regret any inconvenience and want you to know that we are 100-percent committed to safeguarding the data entrusted to us.

If you have any further questions or concerns about this incident, or require assistance enrolling in the free credit monitoring services, please call 877-363-7796, Monday through Friday between 9:00 AM and 9:00 PM Eastern for more information.

Sincerely,



David A. Resnick
Managing Partner
Katz, Sapper & Miller

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, and Virginia: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state law to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Illinois, Maryland, North Carolina, and Rhode Island:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT
(438-4338)
www.ftc.gov/idtheft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- **Equifax** (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)
- **Experian** (<https://www.experian.com/fraud/center.html>)
- **TransUnion** (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>)

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.