



Attorneys at Law

Alabama
Florida
Georgia
Louisiana
Mississippi
South Carolina
Tennessee
Texas
Washington, DC

David Katz

Partner
Direct: 470.427.3726
E-Fax: 470.427.3696
david.katz@arlaw.com

May 24, 2019

[VIA U.S. MAIL AND E-MAIL TO attorneygeneral@doj.nh.gov]

The Office of Attorney General Gordon J. MacDonald
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald,

This Firm represents Aprio LLP (“Aprio”), whose mailing address is 5 Concourse Parkway, Suite 1000, Atlanta, GA 30328. Aprio is a business consulting company and advisory firm that offers advisory, accounting, assurance, tax, and private client services. Pursuant to N.H. Rev. Stat. § 359-C:20(I)(b), we are writing to inform your office of an incident that may have affected the security of personal information relating to one (1) New Hampshire resident. Aprio’s investigation into this event is ongoing, and this notice will be supplemented with any new, significant facts learned after the submission of this notice. By providing this notice, Aprio is not waiving any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data breach notification statute, or personal jurisdiction.

On February 11, 2019, Aprio confirmed that a cyber attacker accessed an employee’s Office 365 e-mail account on or about February 6, 2019, and February 11, 2019. Aprio first learned of the potential security incident on February 11 when an employee in its IT department observed an unusually large number of e-mails being sent from one specific Aprio employee’s e-mail address. Through subsequent investigation, Aprio learned that this particular employee’s mandatory multifactor authentication on his/her mobile device had been inadvertently disabled. The disabled multifactor authentication on this employee’s device enabled the cyber attacker to access this employee’s Office 365 e-mail account. Consequently, the attacker was able to intrude upon Aprio’s Office 365 environment.

Upon discovery, Aprio immediately worked to successfully stop the attacker. Aprio also retained counsel and engaged multiple forensic investigators to research the origin of the security incident as well as to determine the scope of the incident. Aprio’s investigation has been ongoing since it first discovered the incident in February and continues today.

In the early phases of its investigation, Aprio sought to definitively state what e-mails and/or accounts the attacker was able to view or access while intruding on Aprio’s Office 365 environment. To this end, between February 18 and 19, Aprio preserved Unified Audit Logs containing records of activity across all accounts in Aprio’s Office 365 environment. Although the Unified Audit Logs are helpful for detecting unauthorized activity in a user’s account during

specific timeframes, they do not contain enough detail to understand what the attacker did during the timeframe or to what data the attacker had access.

Because the Unified Audit Logs did not contain enough detail to allow Aprio to definitively state what e-mails were viewed by the attacker during the intrusion, Aprio's investigators sought to obtain a higher level of activity detail from Microsoft through its Clutter Logs. It was not until March 20, 2019, that Aprio was able to obtain those Clutter Logs from Microsoft and was able to communicate actively with Microsoft regarding their content. After significant discussion with Microsoft in the days following Aprio's acquisition of the Clutter Logs, however, Microsoft informed Aprio's investigators that the attacker likely had access to all content in the compromised Aprio employee's Office 365 mailbox due to the activity associated with an IMAP client configured to the compromised employee's account on February 7. Therefore, on April 19, Aprio's forensic investigators concluded that the attacker likely had access to all the content in the compromised employee's mailbox.

Once Aprio's investigators concluded the attacker likely had access to all content in the compromised employee's mailbox, it turned its focus to analyzing the potential personal information ("PI") contained within that mailbox that may have been viewed by the attacker. Unfortunately, because a large part of Aprio's business is tax preparation, and because the compromised employee's mailbox contained more than 7,100 .pdf files, the review of compromised data has taken longer than normal. As a result, Aprio's review of affected individuals remains ongoing.

Aprio continues to consult with information technology and security experts and will follow their recommendations to enhance the security of our systems and processes and to ensure that this type of incident will not occur again. Aprio has already implemented additional security measures designed to prevent such an incident from occurring again, including: implementing strict e-mail retention and expiration policies; blocking internal and external communications containing unencrypted personally identifiable information; enhancing existing and implementing additional security controls; implementing additional phishing training and e-mail detection training with improved methods for removal; and planning "white hat" hacking assessments to improve security by exposing potential vulnerabilities before malicious actors can detect and exploit them.

Although Aprio's investigation is ongoing, the investigation thus far has revealed that the following categories of unencrypted personal information were accessed and/or acquired:

- first and last name;
- social security number;
- street address and/or phone number;
- date of birth;
- driver's license number;
- taxpayer identification number;

- IRS PIN number;
- financial account information (such as a checking account number, routing number, and/or PIN number);
- digital signature.


The above types of information were determined to exist in the following types of documents:

- internal and external email communications between Aprio and its clients, including attachments containing personally identifiable information;
- corporate and individual tax returns and their associated schedules;
- corporate and individual tax preparation documents (including tax credit and quarterly payment documentation); and
- documentation used to calculate applicable taxation amounts.

The notification letter to the affected individual (a template of which is enclosed with this notice) will be sent on May 24, 2019. Aprio is providing a free 12-month Experian IdentityWorks membership to each individual affected. This will allow individuals to monitor their credit reports and restore their identities, if necessary.

Should you have any questions regarding this notice or any other aspects of the cybersecurity incident affecting Aprio, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "David Katz", written over the printed name.

David Katz

cc: Mr. Richard Kopelman, Managing Partner and CEO
Encl: Template of breach notification to individuals



5 Concourse Parkway, Suite 1000
Atlanta, GA 30028

May 24, 2019

##E6636-L01-0000005 0001 00000001 *****ALL FOR AADC 159
SAMPLE A SAMPLE - Aprio_Main



APT 1A
123 ANY ST
ANYTOWN, US 12345-6789



NOTICE OF DATA BREACH

Dear Sample A Sample,

Aprio LLP is committed to the highest quality services with the highest level of integrity in dealing with our clients, which is why we are writing to let you know about a data security incident that involves your personally identifiable information.

What Happened?

On February 11, 2019, we discovered that a cyber attacker accessed an employee's Office 365 email account on or about February 6 and 11, 2019. Upon discovery we immediately worked to successfully stop the attacker. Since that time, we have engaged and utilized multiple cybersecurity experts to assist us in a forensic investigation of this incident. The experts have and continue to review the emails, attachments, and other documents exposed during the February 6-11 timeframe in order to identify the individuals affected by this incident.

Based on the results of the investigation and review of the affected emails and attachments conducted thus far, we have determined that your personally identifiable information was accessed and acquired without authorization by an unauthorized third party. We are not able to determine whether the information was further accessed once it was acquired by the unauthorized individuals. To date, we have not received any reports from clients or other potentially affected individuals of identity theft or fraud as a result of this incident.

We are consulting with information technology and security experts and will follow their recommendations to enhance the security of our systems and processes and to ensure that this type of incident will not occur again. We have implemented additional security measures designed to prevent such an incident from occurring again, including implementation of strict email retention and expiration policies, blocking internal and external communications containing unencrypted personally identifiable information, enhancing existing and implementing additional security controls, implementation of additional phishing training and email detection with improved methods for removal, planning "white hat" hacking assessments to improve security by exposing potential vulnerabilities before malicious actors can detect and exploit them.

0000005



E6636-L01

What Information Was Involved

As a result of this incident, an unauthorized person may have accessed and/or acquired some of your personal information, including your:

- first and last name;
- social security number;
- street address and/or phone number;
- date of birth;
- driver's license number;
- taxpayer identification number;
- IRS PIN number;
- financial account information (such as a checking account number, routing number, and/or PIN number);
- digital signature.

The above types of information were determined to exist in the following types of documents:

- internal and external email communications between Aprio and its clients, including attachments containing personally identifiable information;
- corporate and individual tax returns and their associated schedules;
- corporate and individual tax preparation documents (including tax credit and quarterly payment documentation);
- documentation used to calculate applicable taxation amounts.

What We Are Doing To Protect Your Information

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection 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: MM/DD/YYYY (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.yourwebsite.com
- Provide your activation code: ABCDEFGHI

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 ###-###-#### by MM/DD/YYYY. Be prepared to provide engagement number ENGAGEMENT as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARETM: 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 ###-###-####. 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 one year 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.

What You Can Do

We encourage you to remain vigilant with respect to your personal information, and we encourage you to consider the following steps:

- Contact your credit card and other financial companies you have relationships with to alert them that your identity was compromised and to establish additional security on your personal accounts. Closely monitor all financial accounts including credit cards, checking and saving accounts, 401k accounts, etc., by reviewing statements as well as your credit report, and contact the affected financial institution if you see unauthorized activity.
- If you have any accounts where your Social Security number or any other personally identifiable information is your username or password, please switch them to a distinct username or password immediately.
- If you have not yet done so, please file your tax returns as soon as possible. For additional information, contact your local Internal Revenue Service office or call 1-800-908-4490. You can also visit this IRS website which provides information to taxpayers affected by a data breach: <https://www.irs.gov/Individuals/Data-Breach-Information-for-Taxpayers>.
- Monitor your credit report at all three of the national credit reporting agencies. Even if you do not find any suspicious activity on your credit reports, we recommend that you check your credit report periodically.
- The Fair Credit Reporting Act ("FCRA") requires each of the nationwide credit reporting companies — Equifax, Experian, and TransUnion — to provide you with a free copy of your credit report, at your request, once every 12 months. You can order a free copy of your credit report by:
 - o visiting www.annualcreditreport.com;
 - o calling 877-322-8228; or
 - o completing the Annual Credit Report Form on the Federal Trade Commission website at <http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>.

The contact information for all three national credit reporting agencies is listed below.

Equifax	Experian	TransUnion
Phone: 800-685-1111 P.O. Box 740256 Atlanta, GA 30374 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9532 Allen, TX 75013 www.experian.com	Phone: 800-888-4213 P.O. Box 6790 Fullerton, CA 92834 www.transunion.com

0000005



- Consider placing a fraud alert message on your credit file. By placing this alert on your credit file, any company that requests your credit file will receive a message warning them that you may have been a victim of fraud. Companies that receive this alert may request that you provide proof of your identity. This step will help to protect you from accounts being opened or used by anyone other than yourself. If you would like to place a fraud alert on your credit file, call TransUnion at 1-800-680-7289 or request a fraud alert at <https://www.transunion.com/fraud-victim-resource/place-fraud-alert>.
- You have the right to place a security freeze on your credit report. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please be aware, however, that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified, or overnight mail in order for the freeze to be effective. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) social security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze.
- You may also place a security freeze on your credit report online by visiting the below links:
<https://www.experian.com/freeze/center.html>
<https://www.transunion.com/credit-freeze>
<https://www.equifax.com/personal/credit-report-services/>
- If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and the Attorney General's office in your state. You can also obtain information from these sources about additional methods to prevent identity theft. And you can obtain information from the Federal Trade Commission and/or the three national consumer reporting agencies identified above for more information regarding fraud alerts and security freezes. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
1-877-438-4338
www.ftc.gov/idtheft

For More Information

We take the protection of your personal information very seriously and apologize for any inconvenience that this incident may have caused. If you have any questions regarding this notification, please contact Danielle Berg, Aprio Chief Marketing and Communications Officer, at Danielle.Berg@aprio.com or (770) 353-7111.

Sincerely,

Richard Kopelman

Richard Kopelman
Managing Partner and CEO
Aprio, LLP