

March 17, 2023

Office of the Attorney General
Attn: Security Breach Notification
Jeff Karberg
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

VIA ELECTRONIC MAIL

Re: Report on Law Offices of Horwitz & Citro P.A. Data Incident

Dear Mr. Karberg,

We represent Horwitz & Citro P.A. ("H&C"). We write on behalf of our client to report a data incident as required under the Maryland Personal Information Protection Act ("PIPA").

On or about February 19, 2023, an unidentified individual or individuals deployed ransomware within H&C's computer systems. This ransomware encrypted or disabled most of H&C's systems. H&C has learned that during the attack, the attackers downloaded files from H&C's systems that included personally identifiable information. H&C reported the incident to law enforcement and has worked diligently to restore operations and security since the attack.

The data accessed by the attackers was varied and substantial. However, due to the volume of files taken and the loss of logging data resulting from the attack, H&C cannot determine with certainty the exact scope of personal information the attackers may have extracted. At this time H&C is assuming that the data included personally identifiable information. The incident compromised the data of at least one confirmed resident of Maryland and thus H&C is providing this notice.

H&C is cooperating with law enforcement investigating the attack. H&C is also working to strengthen its information security systems to reduce the risk of a similar attack in the future. H&C has provided written and electronic mail notice to potentially affected

individuals including those potentially affected residents of Maryland. A copy of this notice accompanies this letter.

For additional information on this incident, please do not hesitate to contact me.

Very Truly Yours,

A handwritten signature in black ink, appearing to be "A. B." followed by a stylized flourish.

**Form of Notice to Maryland Residents
Notice of Data Breach**

Notice of Data Breach

You are receiving this notification because the Law Offices of Horwitz & Citro P.A. ("H&C") recently experienced a data security incident. Consistent with applicable law, we are providing this notice to potentially affected individuals to explain what occurred and help prevent further harm.

What Happened?

On or about February 19, 2023, an unidentified individual or individuals deployed ransomware within H&C's computer systems. This ransomware encrypted or disabled most of H&C's systems. H&C has learned that during the attack, the attackers downloaded files from H&C's systems that included personally identifiable information. H&C reported the incident to law enforcement and has worked diligently to restore operations and security since the attack.

What Information was Involved?

The data accessed by the attackers was varied and substantial. In some cases, the information may have included full names, social security numbers, financial information, dates of birth, email addresses, telephone numbers, addresses, employee identification numbers, a combination of these data, or other data an individual may have provided to H&C in the past. However, due to the volume of files taken and the loss of logging data resulting from the attack, H&C cannot determine with certainty the exact scope of personal information the attackers may have extracted.

To be safe, if you have provided personal information to H&C in the past, or if your personal information was provided to H&C in the past by another, you should assume that your personally identifiable information was compromised in this incident and take appropriate precautions.

What We Are Doing.

H&C has taken swift action to restore the functionality and security of its data systems following the attack. We are cooperating with law enforcement investigating the attack.

H&C is also working to strengthen our information security systems to reduce the risk of a similar attack in the future.

What You Can Do.

The most important thing you can do in response to this incident is to remain vigilant. Whether you have been affected by this specific breach or not, it is important to regularly review personal account statements and credit reports to ensure no unauthorized activity has occurred. Here are a few warning signs to help you determine whether your personal information may have been used by someone else:

- Receiving a bill for services or items you did not purchase
- Being contacted by a debt collector about debt you do not owe
- Seeing collection notices on your credit report that you do not recognize

Malicious actors may try to trick you into giving them more information using the compromised data. If you receive any suspicious communications, particularly regarding financial matters, you should verify the source so these communications before revealing any personal information. If you are threatened by anyone, you should contact law enforcement.

You may want to change your passwords to various online accounts. If you do change your passwords, your new password should be substantially different from your old password to best ensure security. Remember, it is never a good idea to use the same password from work for your personal or household applications.

State law allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any request you make for new loans, credit, credit or debit cards, mortgages, employment, housing or other services.

If at any time you become 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. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

Credit Report Security Freeze Instructions

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-800-349-9960

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
1-800-680-7289

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

8. If you are not a victim of identity theft, a payment of \$5.00 by check, money order, or credit card (Visa, MasterCard, American Express or Discover only) for the freeze. Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Identity Theft — FTC Contact Information

The Federal Trade Commission is located at 600 Pennsylvania Avenue, NW Washington, DC 20580. If you believe you may have been a victim of identity theft, you may file a complaint with the Federal Trade Commission at: www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338).

Here are a few warning signs to help you determine that whether your personal information may have been used by someone else:

- Receiving a bill for services you did not purchase or receive never used
- Being contacted by a debt collector about debt you do not owe
- Seeing collection notices on your credit report that you do not recognize

If you believe someone else may have used your information, you may wish to consider taking additional steps which are outlined on the Federal Trade Commission's website at www.ftc.gov.

State governments also provide resources on protecting yourself against identity theft. Some examples of these resources are listed below.

Florida Attorney General
Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399
1-866-966-7226

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
410-528-8662

DC Attorney General
400 6th Street NW
Washington, D.C. 20001
(202) 727-3400

Credit Monitoring.

H&C is offering credit monitoring services to certain affected individuals at no cost. To enroll in these services, please contact us at bookkeeper@horwitzcitrolaw.com.

More Information.

For more information, you may call us at (407) 843-7733 or write us at bookkeeper@horwitzcitrolaw.com.

We apologize for any inconvenience this may have caused you.

Sincerely,

Law Offices of Horwitz & Citro, P.A.