

Chambliss, Bahner & Stophel, P.C.
Liberty Tower
605 Chestnut Street, Suite 1700
Chattanooga, TN 37450
chamblisslaw.com



Willa B. Kalaidjian
Direct Dial (423) 757-0207
Direct Fax (423) 508-1207
wkalaidjian@chamblisslaw.com

January 20, 2022

INTENDED FOR ADDRESSEE(S) ONLY

VIA EMAIL

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

Dear Sir or Madam:

We represent the Greater Chattanooga Area Chamber of Commerce (the "Chamber") located at 811 Broad Street, Suite 100, Chattanooga, Tennessee 37402, and are writing to notify your office of a data security incident that may affect the security of personal information relating to one (1) Maryland resident.

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the Chamber does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Security Incident

On or around December 9, 2021, the Chamber experienced a ransomware attack. The Chamber immediately launched an investigation, with the assistance of third-party information technology (IT) recovery, legal and incident management experts, to determine the full nature and scope of this incident and the information subject to the attack. The Chamber, working with its outside consultants, began efforts to (i) eliminate the ongoing threat within the Chamber's systems, (ii) restore the Chamber's systems and operations, and (iii) strengthen system safeguards in an effort to prevent reoccurrence, including segregating the system, resetting account passwords, and installing threat monitoring software. Through these efforts, the Chamber was able to determine that unknown actor(s) gained access to two server drives and downloaded approximately 77 GB of data. The content of the downloaded information was reviewed to determine what personal information may have been contained therein. The Chamber's investigation confirmed that the information contained in the files accessed included name, address, Social Security number, and income-related information for certain individuals affiliated with the Chamber.

Notice to Maryland Resident; Number of Maryland Residents Affected

Written notice will be provided to the one (1) affected Maryland resident in substantially the same form as the letter attached here as **Exhibit A**.

Credit Monitoring and Other Steps Taken and To Be Taken

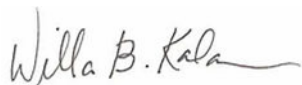
Upon discovering the event, the Chamber moved quickly to investigate and respond to the incident, assess the security of the Chamber's systems, and notify potentially affected individuals. The Chamber is also working to implement additional safeguards and training to its employees. The Chamber is making available credit monitoring services for one year, through Legal Shield's IDShield service, to individuals whose personal information was potentially affected by this incident at no cost to these individuals.

Additionally, the Chamber is providing impacted individuals with guidance on how to better protect against identity theft and fraud. The Chamber is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. In addition, the Chamber notified the Federal Bureau of Investigation and is actively cooperating in their investigation.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at 423-757-0207 or wkalaidjian@chamblisslaw.com.

Sincerely yours,

A handwritten signature in cursive script, appearing to read "Willa B. Kalaidjian".

Willa B. Kalaidjian

EXHIBIT A

[CHAMBER LETTERHEAD]

[DATE]

[INDIVIDUAL NAME]

[STREET]

[CITY], [STATE] [ZIP CODE]

Re: Notice of Data Breach

Dear [NAME]:

I am writing to notify you that some of your personal information was compromised in connection with a security incident recently experienced by the Greater Chattanooga Area Chamber of Commerce (the "Chamber"), and to recommend and offer solutions to help you protect yourself.

What Happened? As you may be aware, the Chamber experienced a ransomware attack on December 9, 2021, and immediately began extensive efforts to (i) eliminate the ongoing threat within the Chamber's systems, (ii) restore the Chamber's systems and operations, and (iii) strengthen system safeguards in an effort to prevent reoccurrence, including segregating the system, resetting account passwords, and installing threat monitoring software. In addition to major investment of time by Chamber staff, the Chamber obtained assistance from outside information technology (IT) recovery, legal, and incident management experts.

What Information Was Involved? We want to notify you that, in the course of our investigation, we discovered that the threat actor who launched the attack obtained copies of accounting records containing the personal information of the Chamber's former and current employees, board chairs and council members. The information contained within certain of those documents included names, social security numbers, driver licenses, addresses, dates of birth, and income-related information. Unfortunately, the Chamber was unable to obtain the return of this information from the threat actor.

What We Are Doing? We deeply regret that the ransomware attack occurred and take the security of personal information seriously. We desire to assist you in protecting yourself against potential misuse of your personal information. **As a precautionary measure, we recommend taking the following steps and utilizing the following resources, which the Chamber has obtained and is making available at no cost to you:**

LegalShield IDShield Credit Monitoring

To help protect your identity, we are offering a complimentary one-year membership of LegalShield's IDShield credit monitoring and identity restoration services. Information on these services and instructions on how to sign up and receive these services is available by visiting <http://LegalShield.com/info/cacoc>. Please note that although the cost of the coverage is shown on the registration page, one full year of coverage is provided courtesy of the Chamber. There will be no charge to the enrollee at checkout.

What You Can Do. In addition to the above complimentary resources that the Chamber has obtained for you, the following resources are generally available:

Credit Reports

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Credit Freeze

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, you may contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-349-9960
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agencies, depending on whether you do so online, by phone, or by mail:

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, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Fraud Alert

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed above.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.marylandattorneygeneral.gov

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For More Information. We hope that you will utilize these resources and recommend that you remain vigilant for any sign of fraud or identity theft involving your personal information. We sincerely apologize for this incident and regret any inconvenience it may cause you. If you need any assistance or have additional questions, please contact Cheryl Millsaps at 423-414-4621.

Sincerely,

Christy Gillenwater
President & CEO