



Burns White Center
48 26th Street
Pittsburgh, PA 15222

t: 412.995.3000

f: 412.995.3300

w: www.burnswwhite.com

Lyle Washowich
Attorney at Law

(412) 995-3004
ldwashowich@burnswwhite.com

CHERRY HILL, NJ

CLEVELAND, OH

HARRISBURG, PA

PHILADELPHIA, PA

PITTSBURGH, PA

PRINCETON, NJ

WHEELING, WV

WILKES-BARRE, PA

WILMINGTON, DE

January 13, 2022

VIA ELECTRONIC SUBMISSION

Massachusetts Director of Consumer Affairs and Business Regulation

RE: Notice of Data Event

Dear Sir or Madam:

We represent Allegheny Financial Group (“Allegheny Financial”), located at 811 Camp Horne Road, Suite 100, Pittsburgh, PA 15237, with respect to the recent data security incident described herein. We are writing on behalf of Allegheny Financial to notify your Office of an incident that may affect the security of certain personal information of approximately seven (7) Massachusetts residents. While the investigation into this event has concluded, this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Allegheny Financial does not waive any rights or defenses regarding the applicability of Massachusetts law, the Massachusetts data breach notification statute, or personal jurisdiction.

Nature of the Data Event

On December 16, 2021, Allegheny Financial became aware that a cybercriminal gained unauthorized access to one of its employee’s e-mail accounts. Allegheny Financial immediately locked the e-mail account, isolated the employee’s device, and launched an investigation into the nature and scope of the incident. The investigation determined that the cybercriminal had access to this employee’s e-mail account. The investigation also revealed that on December 12, 2021 certain files stored within Allegheny Financial’s systems were subject to unauthorized access by the cybercriminal, and sensitive information related to certain customers was part of the information affected.

Allegheny Financial’s investigation determined that the following types of information may have been accessed as a result of this event: customer name, e-mail address(es), account(s), account number(s), account balance(s), and account custodian(s).

Upon discovering that sensitive customer information had been accessed, Allegheny Financial promptly worked to identify the customers whose applicable information had been accessed. At this time, we are unaware of any identity theft or fraud as a result of this incident.

Notice to Massachusetts Residents

On or around January 8, 2022, Allegheny Financial began providing written notice of this incident to the affected customers, including approximately seven (7) Massachusetts residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*.

Allegheny Financial maintains a written information security program for the protection of personal information of residents of Massachusetts.

Other Steps Taken and To Be Taken

Allegheny Financial is providing potentially impacted individual customers with guidance on how to better protect against identity theft and fraud, including 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. Allegheny Financial will also be providing notice of this event to other regulators as may be required under the applicable state or federal laws.

While Allegheny Financial's investigation has found no evidence that customer social security numbers have been accessed as a result of the incident described herein, the written notice to Allegheny Financial's customers includes an offer of complimentary access to twelve (12) months of credit monitoring and identity theft protection services through Aura Identity Guard. Additionally, the written customer notice includes the contact information for a dedicated call center for potentially affected customers to contact with questions or concerns regarding this incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (412) 995-3004.

Very truly yours,

/s/ Lyle Washowich
Lyle Washowich
Burns White LLC

LW/gad

Enclosures

cc (via electronic mail):

Steve Hawbaker, CFO & COO, Allegheny Financial Group
Daniel Inadomi, Esq., Member, Burns White LLC

EXHIBIT A

<<First Name>> << Last Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

January 8, 2022

Re: Notice of Data Breach

Dear <<First Name>> << Last Name>>:

Allegheny Financial Group (“Allegheny Financial”) is writing to notify you of an incident that may affect the privacy of some of your personal information. Allegheny Financial takes the protection of your information very seriously, and although we have no evidence of identity theft or fraud as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On December 16, 2021, Allegheny Financial became aware that a cybercriminal gained unauthorized access to one of its employee’s e-mail accounts. We immediately locked the e-mail account, isolated the employee’s device, and launched an investigation into the nature and scope of the incident. The investigation determined that the cybercriminal had access to this employee’s e-mail account. The investigation also revealed that on December 12, 2021 certain files stored within Allegheny Financial’s systems were subject to unauthorized access by the cybercriminal, and sensitive information related to certain customers was part of the information affected. Upon discovering that sensitive customer information had been accessed, Allegheny Financial promptly worked to identify the customers whose applicable information had been accessed. As a result of these efforts, it is believed that your personal information may have been accessed during this incident.

What Information Was Involved? Our investigation determined your name, e-mail address(es), account(s), account number(s), account balance(s), and account custodian(s) were present in the documents that were identified as accessed by the unauthorized actor(s). At this time, we are unaware of any identity theft or fraud as a result of this incident.

What We Are Doing. Information privacy and security are among our highest priorities. Upon discovering this incident, we immediately took steps to assess the security of our systems and mitigate the impact of this incident, including isolating potentially infected devices, tracking the activity on those devices, and resetting passwords. We also reviewed existing security policies and implemented additional measures, including advanced endpoint monitoring, to further protect information in our care and to ensure that the incident has been contained.

Although we are unaware of any identity theft or fraud as a result of this incident, we are offering you access to twelve (12) months of credit monitoring and identity theft protection services at no cost to you as an added precaution. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Protect Your Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. For the next 12 to 24 months, we encourage you to remain vigilant against incidents of identity theft and fraud. Additionally, we encourage you to review your account statements and monitor your credit reports for suspicious activity and errors. If you suspect fraud in any Allegheny Financial accounts, please immediately report such activity to Allegheny Financial. Please also review the information contained in the attached *Steps You Can Take to Protect Your Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If so, please contact our dedicated assistance line at (412) 536-8015 8:00 am to 5:00 pm Eastern Standard Time, Monday through Friday. You may also write to Allegheny Financial Group at 811 Camp Horne Road, Suite 100, Pittsburgh, PA 15237.

Sincerely,

Steve Hawbaker
Chief Financial Officer and Chief Compliance Officer
Allegheny Financial Group

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at our expense and at no cost to you, in a credit monitoring and identity theft protection service (Identity Guard® Total) for twelve (12) months provided by Aura Identity Guard. Identity Guard® Total provides essential monitoring and protection of not only credit data, but also monitors the Dark Web and alerts you if your Social Security number, credit cards, and bank account numbers are found in unsecure online locations.

Identity Guard® Total features include:

- Dark Web Monitoring
- High Risk Transaction Alerts
- US Based Identity Theft Recovery Assistance
- 3-Bureau Credit Monitoring
- \$1 Million Identity Theft Insurance*
- Bank Account Monitoring
- Account Access via Mobile App
- Anti-Phishing App/Safe Browser Extension

If you wish to take advantage of this monitoring service, you must enroll by May 6, 2022.

How to Enroll: To activate this coverage please visit the Web site listed below and enter the activation code. The activation code is required for enrollment and can only be used one time by the individual addressed.

Web Site: app.identityguard.com/activate/afg
Activation Code: **XXXXXXXXXXXXXX**

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-mail Address
- Activation Code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today.

Monitor Credit Information

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. We recommend periodically obtaining credit reports from each nationwide credit reporting agency and having information relating to fraudulent transactions deleted. 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 listed below directly to request a free copy of your credit report.

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

* Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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, please contact the major consumer reporting agencies using the following information:

Experian

P.O. 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

P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045

www.equifax.com/personal/credit-report-services

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. All of the addresses where you have lived over the prior five (5) 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 a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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 one-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 major consumer reporting agencies using the following information:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft prevention, 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); and 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 about 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 District of Columbia residents, the Attorney General for the District of Columbia may be contacted at 400 6th Street NW, Washington, D.C. 20001; 1-202-727-3400; and <https://oag.dc.gov>.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; 1-888-743-0023; or www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.