



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 16, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

Our office continues to represent AFTRA Retirement Fund (“AFTRA”) located at 261 Madison Avenue, 7th floor, New York, NY 10016-2309. We write to supplement our February 25, 2020 notice to your office concerning an incident that may affect the privacy of personal information related to certain Washington residents. Our prior submission is attached as *Exhibit A*. Notice of this event was also provided via a nationwide press release and through a posting on AFTRA’s home page on February 25, 2020. By providing this notice, AFTRA does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Since providing the initial notice, press release, and web posting, AFTRA continued its extensive internal review of the files and folders that may have been subject to unauthorized access. On September 25, 2020, AFTRA completed its review and produced a list of individuals that may have been impacted. On December 16, 2020, AFTRA began providing notice of this incident to an additional approximate eight thousand two hundred thirty (8,230) Washington residents. The information related to these residents includes name, address, date of birth and Social Security number. Notice is being provided in substantially the same form as the letter attached as *Exhibit B*.

AFTRA is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one year through Kroll at no cost to the individuals. AFTRA is also providing impacted individuals with guidance on how to better protect

Office of the Attorney General

December 16, 2020

Page 2

against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. AFTRA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. AFTRA is also providing notice to other regulators as required.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'J. Boogay', is positioned above the typed name.

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/pls
Enclosure

EXHIBIT A

TO THE

SUPPLEMENTAL

NOTICE



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 25, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent AFTRA Retirement Fund (“AFTRA”) located at 261 Madison Avenue, 7th floor, New York, NY 10016-2309. In 2017, the AFTRA Health Fund merged with the SAG - Producers Health Plan to form the SAG-AFTRA Health Plan. For a period of time following the merger, AFTRA Retirement supported the Health Plan as a business associate.

We are writing to notify your office, on behalf of AFTRA and the SAG-AFTRA Health Plan, of an incident that may affect the security of some personal information relating to five hundred and seventy-three (573) Washington residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, AFTRA does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 28, 2019, AFTRA received an alert of suspicious activity in its environment. AFTRA immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic expert, it was determined that certain files and folders on AFTRA’s network may have been subject to

unauthorized access for periods of time between October 24, 2019 and October 28, 2019. At this time, AFTRA does not have evidence that files containing sensitive information were accessed; however, access to these files could not be ruled out.

AFTRA therefore undertook a time-consuming review of all the files and folders that may have been accessed to determine what sensitive information they may contain. The information that was potentially subject to unauthorized access includes: name, Social Security number, AFTRA number, date of birth, date of death, address and past information about: eligibility, dependent(s), claims, earnings, contributions, and beneficiaries. The data impacted varied by individual.

AFTRA's review of accessible files is ongoing and this notice may be supplemented with new information learned once the review is complete.

Notice to Washington Residents

On or about February 25, 2020 AFTRA began mailing written notice of this incident to all affected individuals for whom it had sufficient address information, which includes approximately five hundred and seventy-three (573) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. In addition, AFTRA posted notice of the incident on its website and issued a press release nationwide on February 25, 2020.

Other Steps Taken and To Be Taken

Upon discovering the event, AFTRA moved quickly to investigate and respond to the incident, assess the security of AFTRA systems, and notify potentially affected individuals. AFTRA is also working to implement additional safeguards and training to its employees. AFTRA is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one year through Kroll, at no cost to these individuals.

Additionally, AFTRA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. AFTRA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. AFTRA is also providing notice to other regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Jeffrey J. Boogay', is written over a light blue horizontal line.

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB:ncl

Enclosure

c.c.: Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188
E-mail: securitybreach@atg.wa.gov
(via email)

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach

Hello <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

AFTRA Retirement Fund (hereafter referred to as “We”, “AFTRA”, “Our”) is writing to advise you of an incident that may affect the security of some of your personal information. As you may recall, in 2017, the AFTRA Health Fund merged with the SAG - Producers Health Plan to form the SAG-AFTRA Health Plan (hereafter referred to as “Health Plan”). For a period of time following the merger, AFTRA Retirement supported the Health Plan as a business associate. We take this incident very seriously and are providing you with information and access to resources so you can better protect against the possibility of misuse of your personal information should you feel it is appropriate to do so.

What Happened? On October 28, 2019, AFTRA received an alert of suspicious activity in its environment. AFTRA immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic expert, it was determined that certain files and folders on AFTRA’s network may have been subject to unauthorized access for periods of time between October 24, 2019 and October 28, 2019. At this time, AFTRA does not have evidence that files containing your information were accessed; however, access to these files could not be ruled out. AFTRA then undertook a time-consuming review of all the files and folders that may have been accessed to determine what sensitive information they may contain.

AFTRA completed an analysis of the contents of the files and folders and prepared a list of potentially impacted individuals whose information was determined to be present and possibly viewable by the unauthorized actor.

What Information Was Involved? The information in the files and folders that was potentially subject to unauthorized access includes: <<b2b_text_1 (Impacted Data)>>.

What We Are Doing. AFTRA takes this incident and the security of information in its care very seriously. AFTRA is reviewing its existing security measures and working to implement additional safeguards to prevent similar incidents from occurring in the future. AFTRA will also notify the Office of Civil Rights at the Department of Health and Human Services and any required state or federal regulators regarding this incident.

As an added precaution, AFTRA is also offering you access to 12 months of complimentary identity monitoring services through Kroll. The cost of this service will be paid for by AFTRA. Instructions on how to activate the identity monitoring services can be found in the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*.

What You Can Do. As a best practice, you should always carefully review your Explanations of Benefits for suspicious or unauthorized activity, and report any instances of fraud to law enforcement. You can also review the attached *Steps You Can Take to Help Protect Against Identity Theft and Fraud* for more information regarding how to further better protect yourself should you feel it appropriate to do so.

For More Information. We understand that you may have questions about the incident that may not be addressed in this letter. If you have additional questions, or need assistance, please call 1-844-936-0060, Monday through Friday, from 9:00 am to 6:30 pm Eastern Time.

The security of personal information is a top priority for AFTRA. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,



Judy Peña
Chief Administrative Officer
AFTRA Retirement Fund

Steps You Can Take to Help Protect Against Identity Theft and Fraud

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

*You have until **May 25, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Monitor Your Accounts.

AFTRA encourages you to remain vigilant against incidents of identity theft, to review your account statements, and to monitor your credit reports and explanation of benefits forms 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.

Security 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, please contact the major consumer reporting agencies listed below:

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Experian

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

Equifax

PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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. 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 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;

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

Place Fraud Alerts.

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 below:

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

File Police Report.

You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Additional information on how to protect your identity.

You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should 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, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, 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 violator. 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 Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 74 Rhode Island residents impacted by this incident.

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/>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Noel Lockridge

From: Colin Scanlon
Sent: Tuesday, February 25, 2020 7:00 PM
To: securitybreach@atg.wa.gov
Cc: Jeff Boogay; Patricia Moore; Noel Lockridge; John Mullen
Subject: Aftra Retirement Fund - Notice of Data Event - WA
Attachments: AFTRA - Notice of Data Event - WA.pdf

Dear Sir or Madam:

Please see the attached notice of data event.

Regards,

Colin Scanlon

Attorney

Mullen Coughlin LLC

1275 Drummers Lane, Suite 302

Wayne, PA 19087

(267) 930-4259 - Office

(570) 881-4987 - Mobile

cscanlon@mullen.law



This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.

EXHIBIT B

TO THE

SUPPLEMENTAL

NOTICE



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach

Hello <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

AFTRA Retirement Fund (hereafter referred to as “We”, “AFTRA”, “Our”) is writing to advise you of an incident that may affect the security of some of your personal information. We take this incident very seriously and are providing you with information and access to resources so you can better protect against the possibility of misuse of your personal information should you feel it is appropriate to do so.

What Happened? On October 28, 2019, AFTRA received an alert of suspicious activity in its environment. AFTRA immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic specialist, it was determined that certain files and folders on AFTRA’s network may have been subject to unauthorized access for periods of time between October 24, 2019 and October 28, 2019. AFTRA notified the media and placed notice of the incident on its website on February 25, 2020. Following these notices, AFTRA continued to review the files that may have been subject to unauthorized access to assess who could be impacted. AFTRA does not have evidence that files containing your information were accessed; however, access to these files could not be ruled out. AFTRA’s internal review of the files and folders was time consuming and completed on September 25, 2020.

What Information Was Involved? The information in the files and folders that was potentially subject to unauthorized access includes: <<b2b_text_1 (Impacted Data)>>.

What We Are Doing. AFTRA takes this incident and the security of information in its care very seriously. AFTRA reviewed its existing security measures and implemented additional safeguards to prevent similar incidents from occurring in the future. AFTRA also notified any required state or federal regulators of this incident.

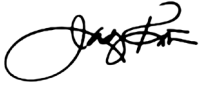
As an added precaution, AFTRA is also offering you access to 12 months of complimentary identity monitoring services through Kroll. The cost of this service will be paid for by AFTRA. Instructions on how to activate the identity monitoring services can be found in the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*.

What You Can Do. As a best practice, you should always carefully review your account records for suspicious or unauthorized activity, and report any instances of fraud to law enforcement. You can also review the attached “*Steps You Can Take to Help Protect Against Identity Theft and Fraud*” for more information regarding how to further protect yourself should you feel it appropriate to do so. We encourage you to remain vigilant against incidents of identity theft, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand that you may have questions about the incident that may not be addressed in this letter. If you have additional questions, or need assistance, please call 1-833-971-3245, Monday through Friday from 9:00 am to 6:30 pm Eastern Time, excluding major U.S. holidays.

The security of personal information is a top priority for AFTRA. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Judy Peña', written in a cursive style.

Judy Peña
Chief Administrative Officer
AFTRA Retirement Fund

Steps You Can Take to Help Protect Against Identity Theft and Fraud

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **April 3, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Monitor Your Accounts.

AFTRA encourages you to remain vigilant against incidents of identity theft, to review your account statements, and to monitor your credit reports and explanation of benefits forms 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.

Security 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, please contact the major consumer reporting agencies listed below:

TransUnion

P.O. Box 2000

Chester, PA 19016

1-800-909-8872

www.transunion.com/credit-freeze

Experian

PO Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/freeze/center.html

Equifax

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

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. 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 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;

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

Place Fraud Alerts.

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 below:

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

File Police Report.

You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Additional information on how to protect your identity.

You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, 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 violator. 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 Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 965 Rhode Island residents impacted by this incident.

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/>.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 25, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent AFTRA Retirement Fund (“AFTRA”) located at 261 Madison Avenue, 7th floor, New York, NY 10016-2309. In 2017, the AFTRA Health Fund merged with the SAG - Producers Health Plan to form the SAG-AFTRA Health Plan. For a period of time following the merger, AFTRA Retirement supported the Health Plan as a business associate.

We are writing to notify your office, on behalf of AFTRA and the SAG-AFTRA Health Plan, of an incident that may affect the security of some personal information relating to five hundred and seventy-three (573) Washington residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, AFTRA does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 28, 2019, AFTRA received an alert of suspicious activity in its environment. AFTRA immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic expert, it was determined that certain files and folders on AFTRA’s network may have been subject to

unauthorized access for periods of time between October 24, 2019 and October 28, 2019. At this time, AFTRA does not have evidence that files containing sensitive information were accessed; however, access to these files could not be ruled out.

AFTRA therefore undertook a time-consuming review of all the files and folders that may have been accessed to determine what sensitive information they may contain. The information that was potentially subject to unauthorized access includes: name, Social Security number, AFTRA number, date of birth, date of death, address and past information about: eligibility, dependent(s), claims, earnings, contributions, and beneficiaries. The data impacted varied by individual.

AFTRA's review of accessible files is ongoing and this notice may be supplemented with new information learned once the review is complete.

Notice to Washington Residents

On or about February 25, 2020 AFTRA began mailing written notice of this incident to all affected individuals for whom it had sufficient address information, which includes approximately five hundred and seventy-three (573) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. In addition, AFTRA posted notice of the incident on its website and issued a press release nationwide on February 25, 2020.

Other Steps Taken and To Be Taken

Upon discovering the event, AFTRA moved quickly to investigate and respond to the incident, assess the security of AFTRA systems, and notify potentially affected individuals. AFTRA is also working to implement additional safeguards and training to its employees. AFTRA is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one year through Kroll, at no cost to these individuals.

Additionally, AFTRA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. AFTRA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. AFTRA is also providing notice to other regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Jeffrey J. Boogay', written in a cursive style.

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB:ncl

Enclosure

c.c.: Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188
E-mail: securitybreach@atg.wa.gov
(via email)

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach

Hello <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

AFTRA Retirement Fund (hereafter referred to as “We”, “AFTRA”, “Our”) is writing to advise you of an incident that may affect the security of some of your personal information. As you may recall, in 2017, the AFTRA Health Fund merged with the SAG - Producers Health Plan to form the SAG-AFTRA Health Plan (hereafter referred to as “Health Plan”). For a period of time following the merger, AFTRA Retirement supported the Health Plan as a business associate. We take this incident very seriously and are providing you with information and access to resources so you can better protect against the possibility of misuse of your personal information should you feel it is appropriate to do so.

What Happened? On October 28, 2019, AFTRA received an alert of suspicious activity in its environment. AFTRA immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic expert, it was determined that certain files and folders on AFTRA’s network may have been subject to unauthorized access for periods of time between October 24, 2019 and October 28, 2019. At this time, AFTRA does not have evidence that files containing your information were accessed; however, access to these files could not be ruled out. AFTRA then undertook a time-consuming review of all the files and folders that may have been accessed to determine what sensitive information they may contain.

AFTRA completed an analysis of the contents of the files and folders and prepared a list of potentially impacted individuals whose information was determined to be present and possibly viewable by the unauthorized actor.

What Information Was Involved? The information in the files and folders that was potentially subject to unauthorized access includes: <<b2b_text_1 (Impacted Data)>>.

What We Are Doing. AFTRA takes this incident and the security of information in its care very seriously. AFTRA is reviewing its existing security measures and working to implement additional safeguards to prevent similar incidents from occurring in the future. AFTRA will also notify the Office of Civil Rights at the Department of Health and Human Services and any required state or federal regulators regarding this incident.

As an added precaution, AFTRA is also offering you access to 12 months of complimentary identity monitoring services through Kroll. The cost of this service will be paid for by AFTRA. Instructions on how to activate the identity monitoring services can be found in the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*.

What You Can Do. As a best practice, you should always carefully review your Explanations of Benefits for suspicious or unauthorized activity, and report any instances of fraud to law enforcement. You can also review the attached *Steps You Can Take to Help Protect Against Identity Theft and Fraud* for more information regarding how to further better protect yourself should you feel it appropriate to do so.

For More Information. We understand that you may have questions about the incident that may not be addressed in this letter. If you have additional questions, or need assistance, please call 1-844-936-0060, Monday through Friday, from 9:00 am to 6:30 pm Eastern Time.

The security of personal information is a top priority for AFTRA. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,



Judy Peña
Chief Administrative Officer
AFTRA Retirement Fund

Steps You Can Take to Help Protect Against Identity Theft and Fraud

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

*You have until **May 25, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Monitor Your Accounts.

AFTRA encourages you to remain vigilant against incidents of identity theft, to review your account statements, and to monitor your credit reports and explanation of benefits forms 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.

Security 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, please contact the major consumer reporting agencies listed below:

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Experian

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

Equifax

PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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. 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 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;

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

Place Fraud Alerts.

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 below:

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

File Police Report.

You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Additional information on how to protect your identity.

You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should 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, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, 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 violator. 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 Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 74 Rhode Island residents impacted by this incident.

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/>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.