



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Kevin M. Mekler
Office: (267) 930-2190
Fax: (267) 930-4771
Email: Kmekler@mullen.law

3001 N. Rocky Point Drive East, Suite 200
Tampa, FL 33607

February 18, 2022

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Welfare & Pension Administration Service, Inc. (“WPAS”), PO Box 34203, Seattle, WA 98124-1203 and are writing to notify your office of an incident that may affect the security of some personal information relating to approximately six (6) Maryland residents. WPAS is a third-party administration firm that specializes in multi-employer benefit plan administration. In order to provide these services, WPAS receives information from its clients, and this notice is being provided on behalf of WPAS and the following entities (collectively referred to as “Clients”) identified in ***Exhibit A*** with the approximate number of impacted individuals included.

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, WPAS 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 Event

On July 21, 2021, WPAS discovered that portions of its computer network were infected with malware that encrypted certain systems. WPAS promptly launched a comprehensive investigation into the nature and scope of the activity and implemented immediate measures to contain the incident. On or about July 28, 2021, the investigation confirmed that certain folders may have been accessed or removed from WPAS’s network; however, the investigation could not definitely confirm what information was accessed or removed. Therefore, WPAS undertook a lengthy, time-intensive, and thorough review of the affected folders to identify the information that was potentially impacted and to whom it related. The initial review completed on or around December 7, 2021, at which time WPAS confirmed the impacted data included information relating to certain individuals. WPAS continued to work through December 20, 2021 to confirm the accuracy of the impacted data and address information for impacted individuals, and to identify the applicable WPAS clients so it could provide accurate notice to individuals and business partners.

While the information is not the same for each affected individual, the potentially impacted information includes name, address, Social Security number, and financial account information.

Notice to Maryland Residents

On or about January 3, 2022, WPAS began providing written notice of this incident to data owners. Subsequently, on or about February 18, 2022, after receiving additional information from clients, WPAS began providing written notice of this incident to affected individuals, including six (6) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***. WPAS also posted notice of this incident on its website, a copy of which is attached here as ***Exhibit C***. This notice may be supplemented if it is determined a significant number of additional Maryland residents will receive notice and at the request of clients.

Other Steps Taken and To Be Taken

Upon discovering the event, WPAS promptly investigated and mitigated potential harm from this incident. WPAS notified the Federal Bureau of Investigation and has been cooperating with the investigation. WPAS worked quickly to confirm what information was impacted, and to which WPAS clients the information belonged so they could be notified. WPAS continues to assess the security of WPAS systems and to enhance existing policies and procedures, including implementing additional safeguards intended to safeguard information and to reduce the likelihood of similar events. WPAS is also working with its business partners to notify impacted individuals.

Although WPAS is not aware of any fraudulent misuse of information from this incident, it is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, WPAS is providing impacted individuals with guidance on how to protect against identity theft and fraud. WPAS 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. WPAS has notified the United States Department of Health of Human Services.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2190.

Very truly yours,



Kevin M. Mekler of
MULLEN COUGHLIN LLC

KMK:rhb
Enclosure

Exhibit *A*

State	Notifying Entity	Approximate Number of Residents
MD	Alaska Painters Trust Funds	1
MD	Alaska Ironworkers Pension Trust	2
MD	Unaffiliated with any third party. Noticed directly by WPAS.	3

Total

6



Exhibit B



Welfare & Pension Administration Service, Inc.

Physical Address: 7525 SE 24th Street, Suite 200, Mercer Island, WA 98040

Mailing Address: PO Box 34203, Seattle, Washington 98124

Phone (206) 441-7574 • Toll-Free (800) 732-1121 • Fax (206) 505-WPAS (9727)

Website: www.wpas-inc.com

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

<<b2b_text_1(NOTICE OF DATA [SECURITY INCIDENT] / [BREACH])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Welfare & Pension Administration Service, Inc. (“WPAS”) is writing to make you aware of a recent incident that may impact some of your information. WPAS is a third-party administration firm that specializes in multi-employer benefit plan administration. We have your information because we provided administrative services to a fund(s) with which you may be associated, including <<b2b_text_2(Fund Name)>>. This notice provides you with information about the incident, our response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On July 21, 2021, WPAS discovered that portions of our computer network were infected with malware that encrypted certain systems. We promptly activated our Incident Response Team, isolated the affected systems, initiated other containment measures, and with the assistance of third-party forensic specialists, launched an investigation into the nature and scope of the incident. On or about July 28, 2021, the investigation confirmed that certain folders may have been accessed or removed from our systems without authorization. We therefore undertook a lengthy, time-intensive, and thorough review of the potentially impacted folders to identify the information that was potentially impacted and to whom it related. We completed these preliminary efforts on or around December 7, 2021, at which time we began the process of reviewing our internal files and systems to identify accurate address information for the potentially impacted individuals. After this process was completed on or around December 20, 2021, WPAS worked with its partner funds to provide notification to potentially impacted individuals as quickly as possible.

What Information Was Involved? Our investigation determined that the information related to you that may have been potentially affected includes your <<b2b_text_3(Name, Data Elements)>><<b2b_text_4(Data Elements cont)>>. Importantly, there is no indication that your specific information was accessed or misused. However, we are notifying potentially impacted individuals out of an abundance of caution.

What We Are Doing. Information security is one of WPAS’s highest priorities, and we have security measures in place to help protect information in our care. Upon discovering this incident, we promptly took steps to respond, including taking steps to mitigate the event by resetting passwords across the network and bringing in third-party forensic specialists to assist with the investigation and remediation. Further, we notified federal law enforcement regarding this event. Moreover, following our investigation, WPAS has taken steps to further secure its environment, and is reviewing and enhancing existing policies and procedures and implementing additional safeguards to further secure the information in our systems and reduce the likelihood of a similar future event. We are also notifying relevant regulatory authorities as required.

As an added precaution, WPAS is offering you access to twelve (12) months of identity monitoring services through Kroll at no cost to you. You will find information on how to activate these services in the enclosed “*Steps You Can Take To Help Protect Your Information.*” We encourage you to activate these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached “*Steps You Can Take To Help Protect Your Information.*”

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated assistance line at (855) 568-2075, which is available Monday through Friday, from 8:00 a.m. to 5:00 p.m. Pacific Time, excluding major U.S. holidays. You may also write to WPAS at PO Box 34203, Seattle, WA 98124-1203.

We take this incident very seriously and sincerely regret any inconvenience or concern it may cause you.

Sincerely,

Privacy Team

Welfare & Pension Administration Service, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate your Identity Monitoring

Visit wpas.kroll.com to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and 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 bureaus 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 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 [4] Rhode Island residents impacted by this incident.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

Exhibit C

UPDATED 02/18/2022

ABOUT THE DATA PRIVACY EVENT

Welfare & Pension Administration Service, Inc. (“WPAS”) is a third-party administration firm that specializes in multi-employer benefit plan administration. WPAS is providing notice of a recent incident that may impact some information of members of some plans WPAS administers. This notice provides you with information about the incident, our response, and steps you may take to protect your personal information, should you feel it necessary.

What Happened? On July 21, 2021, WPAS discovered that portions of our computer network were infected with malware that affected certain systems. We promptly activated our Incident Response Team, isolated the affected systems, initiated other containment measures, and with the assistance of third-party forensic specialists, launched an investigation into the nature and scope of the incident. On or about July 28, 2021, the investigation confirmed that certain folders may have been accessed or removed from our system. WPAS therefore undertook a lengthy, time-intensive, and thorough review of the affected folders to identify the information that was potentially impacted and to whom it related. On or around December 20, 2021, this process was completed and we have been working with our client funds to provide notification to potentially impacted individuals as quickly as possible.

What Information Was Involved? While the specific impacted information varies by individual; our investigation determined that the information which may have been impacted includes individual name, date of birth, Social Security number, driver’s license number, passport number, employer identification number, financial account information and payment card information, electronic or digital signature, medical claims information, medical treatment or diagnosis information, prescription information, health insurance identification number, and health insurance group number. Importantly, there is no indication specific information was accessed or misused. However, together with and on behalf of our client funds, we are providing notice of this incident.

What We Are Doing. Information security is one of WPAS’s highest priorities, and we have security measures in place to protect information in our care. Upon discovering this incident, we promptly took steps to mitigate potential harm from the event. We have reset passwords across the network, brought in third-party forensic specialists to assist with the investigation and remediation, and notified federal law enforcement of this event. WPAS is continuing to review and enhance our existing policies and procedures and is implementing additional safeguards to further secure the information in our systems and reduce the likelihood of a similar future event. We are also assisting our client funds with notifying relevant regulatory authorities.

As an added precaution, WPAS is offering access to credit monitoring and identity protection services through Kroll, at no cost to individuals. You will find information on how to activate these services in the below “*Steps Individuals Can Take To Help Protect Information.*”

What You Can Do. WPAS is not aware of any fraudulent misuse of information. As a general precaution, we encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and to detect errors. Individuals can also review the information contained in the attached “*Steps Individuals Can Take To Help Protect Information.*”

For More Information. If you have additional questions or concerns, please call our dedicated assistance line at (855) 568-2075, which is available Monday through Friday, from 8:00 a.m. to 5:00 p.m. Pacific Time. You may also write to WPAS at PO Box 34203, Seattle, WA 98124-1203.

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT INFORMATION

Credit Monitoring

Visit wpas.kroll.com to activate and take advantage of your identity monitoring services.

You have until May 19, 2022 to activate your identity monitoring services.

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov. *For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and 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 bureaus 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 New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>. *For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. *For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.