



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Richard Aponte-Boyd
Office: (267) 930-4888
Fax: (267) 930-4771
Email: raponte@mullen.law

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

May 3, 2023

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

To Whom It May Concern:

We represent The Metropolitan Opera (“the Met”) located at 30 Lincoln Center Plaza, New York, NY 10023, and write to notify your office of an incident that may affect the security of certain personal information relating to seven hundred fifty-six (756) Maryland residents. By providing this notice, the Met 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 December 6, 2022, the Met identified suspicious activity related to its computer systems. The Met immediately took steps to secure their network and brought in a team of third-party specialists information to help the Met get its systems back up and running and to determine the nature and scope of the suspicious activity. Through an investigation conducted by third-party specialists, the Met learned that an unknown actor gained access to certain of their systems between September 30, 2022 and December 6, 2022 and accessed or took certain information from those systems. The Met completed a review of the contents of those files to determine what information was contained therein and to whom it related.

The information that could have been subject to unauthorized access includes name, financial account information, tax identification number, Social Security number, payment card information, passport number, and driver’s license number.

Notice to Maryland Residents

On May 3, 2023, the Met provided written notice of this incident to seven hundred fifty-six (756) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, the Met moved quickly to investigate and respond to the incident, assess the security of the Met systems, and identify potentially affected individuals. Further, The Met notified federal law enforcement regarding the event. The Met is also working to implement additional safeguards and training to its employees. The Met 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, the Met 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. The Met 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.

The Met is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4888.

Very truly yours,



Richard Aponte-Boyd of
MULLEN COUGHLIN LLC

RAB/kzf
Enclosure

EXHIBIT A

The Metropolitan Opera

<<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 (SubjectLine)>>

Dear <<First_Name>> <<Last_Name>>,

The Metropolitan Opera (“the Met”) writes to inform you of a recent event that may impact the privacy of some of your information. We are not aware of any misuse of your information, but we are providing you with this letter as a precaution, to inform you of the event, our response, and steps you may take to help protect your information, should you feel it is necessary to do so.

What Happened? On December 6, 2022, the Met identified suspicious activity related to its computer systems. We immediately took steps to secure our network and brought in a team of information technology specialists to help the Met get its systems back up and running and to determine the nature and scope of the suspicious activity. Through an investigation conducted by third party forensic specialists, we learned that an unknown actor gained access to our systems between September 30, 2022 and December 6, 2022 and accessed or took certain information from those systems. We have completed a review of the contents of those files to determine what information was contained therein and to whom it related. We are notifying you because your information was contained in the potentially impacted files.

What Information Was Involved? The information contained within the files concerned included your <<b2b_Text_2 (Impacted Information)>>.

What We Are Doing. The confidentiality, privacy, and security of information within our care is among the Met’s highest priorities. Upon learning of the event, we took immediate steps to secure our environment and investigate the activity. We commenced an investigation that included working with an outside team of specialists to understand the nature and scope of the event. We also notified federal law enforcement about this event and have cooperated with their investigation. As part of our ongoing commitment to the security of information, we are also reviewing and further strengthening our systems setup, policies and procedures.

Although we do not have any evidence of identity theft or fraud as a result of this incident, we are offering complimentary Identity Monitoring services through Kroll for 12 months as an added precaution. If you wish to avail yourself of these services, you will need to activate using the instruction enclosed with this letter, as we are unable to activate them on your behalf. Please note that the monitoring service may identify results linked to other events which have no connection whatsoever with this incident.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and monitor your free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You may also activate the complimentary identity monitoring services we are offering to you.

For More Information. If you have additional questions, you may call our dedicated assistance line at (866) 347-9208, available Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding U.S. holidays). You may also write to the Metropolitan Opera at 30 Lincoln Center, New York, NY 10023.

Sincerely,

The Metropolitan Opera

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate Your Identity Monitoring Services

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

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

Membership Number: <<Membership Number (S_N)>>

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



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 help 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.

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	800-916-8800
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 <https://www.marylandattorneygeneral.gov/>.

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 161 Rhode Island residents impacted by this incident.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Richard Aponte-Boyd
Office: (267) 930-4888
Fax: (267) 930-4771
Email: raponte@mullen.law

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

May 22, 2023

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: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent The Metropolitan Opera (“the Met”) located at 30 Lincoln Center Plaza, New York, NY 10023, and write to supplement our May 4, 2023 notice to your office (the “May 4 Notice”). The May 4 Notice is attached hereto as ***Exhibit A***. By providing this notice, the Met 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 December 6, 2022, the Met identified suspicious activity related to its computer systems. The Met immediately took steps to secure their network and brought in a team of third-party specialists information to help the Met get its systems back up and running and to determine the nature and scope of the suspicious activity. Through an investigation conducted by third-party specialists, the Met learned that an unknown actor gained access to certain of their systems between September 30, 2022 and December 6, 2022 and accessed or took certain information from those systems. The Met completed a review of the contents of those files to determine what information was contained therein and to whom it related.

The Met began notifying individuals on May 4, 2023, that the information that could have been subject to unauthorized access includes name, financial account information, tax identification number, Social Security number, payment card information, passport number, and driver’s license number.

Notice to Maryland Residents

As noted above, on May 4, 2023, the Met began providing written notice to potentially impacted individuals of this incident. This notice included notice to seven hundred fifty-six (756) Maryland residents. On May 22, 2023, the Met continued providing notice of this incident to potentially impacted individuals including an additional forty-two (42) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit B**. The total number of Maryland residents notified of this incident is seven hundred ninety-eight (798).

Other Steps Taken and To Be Taken

Upon discovering the event, the Met moved quickly to investigate and respond to the incident, assess the security of the Met systems, and identify potentially affected individuals. Further, The Met notified federal law enforcement regarding the event. The Met is also working to implement additional safeguards and training to its employees. The Met 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, the Met 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. The Met 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.

The Met is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4888.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Richard Aponte-Boyd".

Richard Aponte-Boyd of
MULLEN COUGHLIN LLC

RAB/kzf
Enclosure

EXHIBIT A



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Richard Aponte-Boyd
Office: (267) 930-4888
Fax: (267) 930-4771
Email: raponte@mullen.law

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

May 3, 2023

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

To Whom It May Concern:

We represent The Metropolitan Opera (“the Met”) located at 30 Lincoln Center Plaza, New York, NY 10023, and write to notify your office of an incident that may affect the security of certain personal information relating to seven hundred fifty-six (756) Maryland residents. By providing this notice, the Met 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 December 6, 2022, the Met identified suspicious activity related to its computer systems. The Met immediately took steps to secure their network and brought in a team of third-party specialists information to help the Met get its systems back up and running and to determine the nature and scope of the suspicious activity. Through an investigation conducted by third-party specialists, the Met learned that an unknown actor gained access to certain of their systems between September 30, 2022 and December 6, 2022 and accessed or took certain information from those systems. The Met completed a review of the contents of those files to determine what information was contained therein and to whom it related.

The information that could have been subject to unauthorized access includes name, financial account information, tax identification number, Social Security number, payment card information, passport number, and driver’s license number.

Notice to Maryland Residents

On May 3, 2023, the Met provided written notice of this incident to seven hundred fifty-six (756) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, the Met moved quickly to investigate and respond to the incident, assess the security of the Met systems, and identify potentially affected individuals. Further, The Met notified federal law enforcement regarding the event. The Met is also working to implement additional safeguards and training to its employees. The Met 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, the Met 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. The Met 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.

The Met is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4888.

Very truly yours,



Richard Aponte-Boyd of
MULLEN COUGHLIN LLC

RAB/kzf
Enclosure

EXHIBIT A

The Metropolitan Opera

<<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 (SubjectLine)>>

Dear <<First_Name>> <<Last_Name>>,

The Metropolitan Opera (“the Met”) writes to inform you of a recent event that may impact the privacy of some of your information. We are not aware of any misuse of your information, but we are providing you with this letter as a precaution, to inform you of the event, our response, and steps you may take to help protect your information, should you feel it is necessary to do so.

What Happened? On December 6, 2022, the Met identified suspicious activity related to its computer systems. We immediately took steps to secure our network and brought in a team of information technology specialists to help the Met get its systems back up and running and to determine the nature and scope of the suspicious activity. Through an investigation conducted by third party forensic specialists, we learned that an unknown actor gained access to our systems between September 30, 2022 and December 6, 2022 and accessed or took certain information from those systems. We have completed a review of the contents of those files to determine what information was contained therein and to whom it related. We are notifying you because your information was contained in the potentially impacted files.

What Information Was Involved? The information contained within the files concerned included your <<b2b_Text_2 (Impacted Information)>>.

What We Are Doing. The confidentiality, privacy, and security of information within our care is among the Met’s highest priorities. Upon learning of the event, we took immediate steps to secure our environment and investigate the activity. We commenced an investigation that included working with an outside team of specialists to understand the nature and scope of the event. We also notified federal law enforcement about this event and have cooperated with their investigation. As part of our ongoing commitment to the security of information, we are also reviewing and further strengthening our systems setup, policies and procedures.

Although we do not have any evidence of identity theft or fraud as a result of this incident, we are offering complimentary Identity Monitoring services through Kroll for 12 months as an added precaution. If you wish to avail yourself of these services, you will need to activate using the instruction enclosed with this letter, as we are unable to activate them on your behalf. Please note that the monitoring service may identify results linked to other events which have no connection whatsoever with this incident.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and monitor your free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You may also activate the complimentary identity monitoring services we are offering to you.

For More Information. If you have additional questions, you may call our dedicated assistance line at (866) 347-9208, available Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding U.S. holidays). You may also write to the Metropolitan Opera at 30 Lincoln Center, New York, NY 10023.

Sincerely,

The Metropolitan Opera

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate Your Identity Monitoring Services

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

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

Membership Number: <<Membership Number (S_N)>>

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



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 help 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.

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	800-916-8800
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 <https://www.marylandattorneygeneral.gov/>.

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 161 Rhode Island residents impacted by this incident.

EXHIBIT B

The Metropolitan Opera

<<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 (SubjectLine)>>

Dear <<First_Name>> <<Last_Name>>,

The Metropolitan Opera (“the Met”) writes to inform you of a recent event that may impact the privacy of some of your information. We are not aware of any misuse of your information, but we are providing you with this letter as a precaution, to inform you of the event, our response, and steps you may take to help protect your information, should you feel it is necessary to do so.

What Happened? On December 6, 2022, the Met identified suspicious activity related to its computer systems. We immediately took steps to secure our network and brought in a team of information technology specialists to help the Met get its systems back up and running and to determine the nature and scope of the suspicious activity. Through an investigation conducted by third party forensic specialists, we learned that an unknown actor gained access to our systems between September 30, 2022 and December 6, 2022 and accessed or took certain information from those systems. We have completed a review of the contents of those files to determine what information was contained therein and to whom it related. We are notifying you because your information was contained in the potentially impacted files.

What Information Was Involved? The information contained within the files concerned included your <<b2b_Text_2 (Impacted Information)>>.

What We Are Doing. The confidentiality, privacy, and security of information within our care is among the Met’s highest priorities. Upon learning of the event, we took immediate steps to secure our environment and investigate the activity. We commenced an investigation that included working with an outside team of specialists to understand the nature and scope of the event. We also notified federal law enforcement about this event and have cooperated with their investigation. As part of our ongoing commitment to the security of information, we are also reviewing and further strengthening our systems setup, policies and procedures.

Although we do not have any evidence of identity theft or fraud as a result of this incident, we are offering complimentary Identity Monitoring services through Kroll for 12 months as an added precaution. If you wish to avail yourself of these services, you will need to activate using the instruction enclosed with this letter, as we are unable to activate them on your behalf. Please note that the monitoring service may identify results linked to other events which have no connection whatsoever with this incident.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and monitor your free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You may also activate the complimentary identity monitoring services we are offering to you.

For More Information. If you have additional questions, you may call our dedicated assistance line at (866) 347-9208, available Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding U.S. holidays). You may also write to the Metropolitan Opera at 30 Lincoln Center, New York, NY 10023.

Sincerely,

The Metropolitan Opera

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate Your Identity Monitoring Services

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

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

Membership Number: <<Membership Number (S_N)>>

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



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 help 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.

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	800-916-8800
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 <https://www.marylandattorneygeneral.gov/>.

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 161 Rhode Island residents impacted by this incident.