WILSON ELSER

January 21, 2025

Dominik Cvitanovic
(504)-702-1710
Dominik.Cvitanovic@wilsonelser.com

Via regular and certified mail

RI Office of the Attorney General
150 South Main Street
Providence, RI 02903

Re: Cybersecurity Incident Involving Wolf Haldenstein Adler Freeman & Herz LLP
Wilson Elser File No: 23357.00007

Dear Attorney General Neronha :

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Wolf Haldenstein Adler Freeman & Herz LLP ("Wolf Haldenstein") a law firm headquartered at 270 Madison Avenue, New York, New York 10016, with respect to a cybersecurity incident that was first discovered by Wolf Haldenstein on April 18, 2024 (hereinafter, the "Incident"). Wolf Haldenstein takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve as notice of the nature of the Incident, what information may have been compromised, the number of Rhode Island residents being notified, and the steps that Wolf Haldenstein has taken in response to the Incident. By providing this notice, Wolf Haldenstein does not waive any rights or defenses regarding the applicability of Rhode Island law, the applicability of Rhode Island data event notification statute, or personal jurisdiction.

1. Nature of the Incident

On December 13, 2023, Wolf Haldenstein detected suspicious activity in its network environment. Upon discovery of this incident, Wolf Haldenstein promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Wolf Haldenstein learned that an unauthorized actor potentially accessed certain files and data stored within its network. Wolf Haldenstein also conducted an examination of its systems and networks using all information available to determine the potential impact and the security of data housed on its servers.

Wolf Haldenstein subsequently undertook a time-consuming and detailed review of the data stored on the servers at the time of this incident to understand to whom that data relates. On December 3, 2024, Wolf Haldenstein identified a subset of potentially affected persons but Wolf Haldenstein was unable to locate address information to provide direct notice to the subset of potentially

impacted individuals.

The following types of information may have been impacted: name, Social Security number, employee identification number, medical diagnosis, and medical claim information.

2. Number of Rhode Island residents affected.

A total of 16,071 Rhode Island residents may have been potentially impacted by this incident. A substitute notice was published on January 13, 2025. A copy of the notice is attached as **Exhibit "A."**

3. Steps taken in response to the Incident.

Wolf Haldenstein takes this event and the security of personal information in its care very seriously. Upon learning of this event, Wolf Haldenstein moved quickly to investigate and respond to the event and notify potentially affected individuals. As part of its ongoing commitment to the security of information, Wolf Haldenstein reviewed and enhanced its existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. Wolf Haldenstein is also offering complimentary credit monitoring to individuals who believe they may have been affected by this incident and are interested in this service.

4. Contact information

Wolf Haldenstein remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Dominik.Cvitanovic@wilsonelser.com or 504-702-1710.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Dominik J. Cvitanovic, Esq.

EXHIBIT A

Website Notice

UPDATED NOTICE OF DATA PRIVACY EVENT

January 10, 2025 – Wolf Haldenstein Adler Freeman & Herz LLP ("Wolf Haldenstein") is providing updated notice of an event that may affect the privacy of certain individuals' information. Wolf Haldenstein takes this incident very seriously and is providing information about the incident, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On December 13, 2023, Wolf Haldenstein detected suspicious activity in its network environment. Upon discovery of this incident, Wolf Haldenstein promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Wolf Haldenstein learned that an unauthorized actor accessed certain files and data stored within its network. Wolf Haldenstein also conducted an examination of its systems and networks using all information available to determine the potential impact and the security of data housed on its servers.

Wolf Haldenstein subsequently undertook a time-consuming and detailed review of the data stored on the servers at the time of this incident to understand to whom that data relates. On December 3, 2024, Wolf Haldenstein identified a subset of potentially affected persons but Wolf Haldenstein was unable to locate address information to provide direct notice to the subset of potentially impacted individuals.

What Information Was Involved? While we have no evidence that any personal information has been misused, we are notifying you and providing information and resources to help protect your personal information. The following types of information may have been potentially impacted: name, Social Security number, employee identification number, medical diagnosis, and medical claim information.

What Wolf Haldenstein is Doing. Wolf Haldenstein takes this event and the security of personal information in its care very seriously. Upon learning of this event, Wolf Haldenstein moved quickly to investigate and respond to the event and notify potentially affected individuals. As part of its ongoing commitment to the security of information, Wolf Haldenstein reviewed and enhanced its existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. Wolf Haldenstein is also offering complimentary credit monitoring to individuals who believe they may have been affected by this incident and are interested in this service.

What You Can Do. Wolf Haldenstein encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits forms and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

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 may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

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 fraud alert or 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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; 1-202-727-3400; 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/.

Website Notice

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; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 16,071 Rhode Island residents impacted by this event.

For More Information. If you have questions about receiving complimentary credit monitoring or would like additional information, you may call Wolf Haldenstein's assistance line at 1-(800)-650-5752, between the hours of 9 a.m. to 5 p.m. Eastern time, Monday through Friday. This excludes all major U.S. holidays.

WILSON ELSER

January 21, 2025

Dominik Cvitanovic
(504)-702-1710
Dominik.Cvitanovic@wilsonelser.com

Via regular and certified mail

RI Office of the Attorney General
150 South Main Street
Providence, RI 02903

Re: Cybersecurity Incident Involving Wolf Haldenstein Adler Freeman & Herz LLP
Wilson Elser File No: 23357.00007

Dear Attorney General Neronha :

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Wolf Haldenstein Adler Freeman & Herz LLP ("Wolf Haldenstein") a law firm headquartered at 270 Madison Avenue, New York, New York 10016, with respect to a cybersecurity incident that was first discovered by Wolf Haldenstein on April 18, 2024 (hereinafter, the "Incident"). Wolf Haldenstein takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve as notice of the nature of the Incident, what information may have been compromised, the number of Rhode Island residents being notified, and the steps that Wolf Haldenstein has taken in response to the Incident. By providing this notice, Wolf Haldenstein does not waive any rights or defenses regarding the applicability of Rhode Island law, the applicability of Rhode Island data event notification statute, or personal jurisdiction.

1. Nature of the Incident

On December 13, 2023, Wolf Haldenstein detected suspicious activity in its network environment. Upon discovery of this incident, Wolf Haldenstein promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Wolf Haldenstein learned that an unauthorized actor potentially accessed certain files and data stored within its network. Wolf Haldenstein also conducted an examination of its systems and networks using all information available to determine the potential impact and the security of data housed on its servers.

Wolf Haldenstein subsequently undertook a time-consuming and detailed review of the data stored on the servers at the time of this incident to understand to whom that data relates. On December 3, 2024, Wolf Haldenstein identified a subset of potentially affected persons but Wolf Haldenstein was unable to locate address information to provide direct notice to the subset of potentially

impacted individuals.

The following types of information may have been impacted: name, Social Security number, employee identification number, medical diagnosis, and medical claim information.

2. Number of Rhode Island residents affected.

A total of 16,071 Rhode Island residents may have been potentially impacted by this incident. A substitute notice was published on January 13, 2025. A copy of the notice is attached as **Exhibit "A."**

3. Steps taken in response to the Incident.

Wolf Haldenstein takes this event and the security of personal information in its care very seriously. Upon learning of this event, Wolf Haldenstein moved quickly to investigate and respond to the event and notify potentially affected individuals. As part of its ongoing commitment to the security of information, Wolf Haldenstein reviewed and enhanced its existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. Wolf Haldenstein is also offering complimentary credit monitoring to individuals who believe they may have been affected by this incident and are interested in this service.

4. Contact information

Wolf Haldenstein remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Dominik.Cvitanovic@wilsonelser.com or 504-702-1710.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Dominik J. Cvitanovic, Esq.

EXHIBIT A

Website Notice

UPDATED NOTICE OF DATA PRIVACY EVENT

January 10, 2025 – Wolf Haldenstein Adler Freeman & Herz LLP ("Wolf Haldenstein") is providing updated notice of an event that may affect the privacy of certain individuals' information. Wolf Haldenstein takes this incident very seriously and is providing information about the incident, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On December 13, 2023, Wolf Haldenstein detected suspicious activity in its network environment. Upon discovery of this incident, Wolf Haldenstein promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Wolf Haldenstein learned that an unauthorized actor accessed certain files and data stored within its network. Wolf Haldenstein also conducted an examination of its systems and networks using all information available to determine the potential impact and the security of data housed on its servers.

Wolf Haldenstein subsequently undertook a time-consuming and detailed review of the data stored on the servers at the time of this incident to understand to whom that data relates. On December 3, 2024, Wolf Haldenstein identified a subset of potentially affected persons but Wolf Haldenstein was unable to locate address information to provide direct notice to the subset of potentially impacted individuals.

What Information Was Involved? While we have no evidence that any personal information has been misused, we are notifying you and providing information and resources to help protect your personal information. The following types of information may have been potentially impacted: name, Social Security number, employee identification number, medical diagnosis, and medical claim information.

What Wolf Haldenstein is Doing. Wolf Haldenstein takes this event and the security of personal information in its care very seriously. Upon learning of this event, Wolf Haldenstein moved quickly to investigate and respond to the event and notify potentially affected individuals. As part of its ongoing commitment to the security of information, Wolf Haldenstein reviewed and enhanced its existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. Wolf Haldenstein is also offering complimentary credit monitoring to individuals who believe they may have been affected by this incident and are interested in this service.

What You Can Do. Wolf Haldenstein encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits forms and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

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 may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

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 fraud alert or 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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; 1-202-727-3400; 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/.

Website Notice

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; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 16,071 Rhode Island residents impacted by this event.

For More Information. If you have questions about receiving complimentary credit monitoring or would like additional information, you may call Wolf Haldenstein's assistance line at 1-(800)-650-5752, between the hours of 9 a.m. to 5 p.m. Eastern time, Monday through Friday. This excludes all major U.S. holidays.