June 2, 2025

Via Email: SecurityBreach@atg.wa.gov

Washington Attorney General

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, New York 10019-6022
United States of America

Direct line +1 212 318 3382
david.kessler@nortonrosefulbright.com

Tel +1 212 318 3000
Fax +1 212 318 3400

Re: Supplemental Notice of Data Security Incident (Submission A33410)

Dear Sir or Madam:

I am writing on behalf of our client, Kronick Moskovitz Tiedemann & Girard ("Kronick"), to supplement Kronick's initial notification of a cybersecurity incident to your office.

Kronick is mailing notification letters via First Class Mail to additional Washington residents whose personal information was involved (for a new total of 9892 Washington residents).

Appendix A (attached) contains the names of the Kronick clients who have directed Kronick to provide notice to your office on their behalf. If you have any questions or need further information regarding the incident, please do not hesitate to contact me.

Respectfully submitted,

David Kessler

David Kessler

APPENDIX A

NuWest Group Holdings, LLC
325 118th Ave SE #300
Bellevue, WA 98005

May 23, 2025

Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, New York 10019-6022
United States of America

Direct line +1 212 318 3382
david.kessler@nortonrosefulbright.com

Tel +1 212 318 3000
Fax +1 212 318 3400

Via Portal

Washington Attorney General

Re: Legal Notice of Data Security Incident

Dear Sir or Madam:

I am writing on behalf of my client, Kronick Moskovitz Tiedemann & Girard ("Kronick") to inform you of a data security incident that may have involved personal information belonging to 9,862 Washington residents.

Kronick is a full-service law firm serving public and private clients throughout California. Due to the nature of this work, Kronick is given access to certain personal information of its clients and other individuals related to their matters in the provision of its legal services.

On August 6, 2024, Kronick detected unauthorized access to its network from an unknown third party. At the time of the incident, Kronick had multiple security measures in place, including Multi-Factor Authentication ("MFA") protecting remote access and user workstation logins. Additionally, Kronick had Endpoint Detection and Response ("EDR") software deployed on all servers and endpoints, which blocked the majority of the unauthorized actor's encryption efforts during the attack.

Once Kronick detected the incident, Kronick's IT Team immediately disconnected systems, reset all user passwords, and disabled and reset all service accounts. Additionally, Kronick enhanced MFA requirements and added Cloudflare protection via a DNS proxy to further strengthen system defenses. Kronick has also since deployed additional layers of EDR on all endpoints and rebuilt systems from backups, which were not impacted.

However, while Kronick was able to prevent the unauthorized user from encrypting Kronick's systems in any material way, the unauthorized user was able to exfiltrate data from Kronick's IT systems without detection. The party claiming responsibility for the incident temporarily posted the data it took on the dark web, an encrypted area of the internet that is not indexed by search engines though accessible with special tools and software. In turn, Kronick engaged Norton Rose Fulbright, which began an investigation and engaged leading third-party cybersecurity and forensic experts to assist. Kronick notified law enforcement of the incident. Kronick's team had the information taken down, retrieved it from the unauthorized actor, and received assurances that all unauthorized copies of the data have been deleted. The data is no longer posted on the dark web and, at this time, Kronick has no reason to believe this data was retained by the unauthorized actor or that any additional data was exfiltrated.

Kronick also conducted a thorough review of the data impacted by this issue to identify what information was involved and to identify individuals to whom the data related. The review of data identified that 9,862 Washington residents were impacted by this issue. That includes individuals whose data was in Kronick's possession because of the legal work they do for other companies

and organizations. The organizations that have authorized Kronick to provide notice to you are attached as Appendix “A”.

Kronick had previously mailed notification letters to 3 Washington residents potentially impacted by this incident on January 27, 2025, 2 Washington residents on March 28, 2025, and 169 Washington residents on April 28, 2025. Today, May 23, 2025, Kronick subsequently mailed notification letters to an additional 9,688 Washington residents, thereby meeting the regulatory notification threshold for the Washington Attorney General. Kronick will be offering 24 months of complimentary credit monitoring and fraud protection services. Kronick is also providing a toll-free telephone number for the recipients to provide support and answer additional questions regarding the incident. Attached is a copy of the form notice letter that was sent today.

If you have any questions or need further information regarding the incident, please do not hesitate to contact me.

Respectfully submitted,

David Kessler

David Kessler

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

KRONICK
MOSKOVITZ
TIEDEMANN
& GIRARD

N3830-L05-0000001 P001 T00001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L05 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

May 23, 2025

Re: Notice of Data Security Incident

Dear Sample,

Kronick Moskovitz Tiedemann & Girard ("Kronick"), a full-service law firm serving clients throughout California, was recently the target of a cybersecurity incident. Kronick is writing to inform you that the incident involved some of your personal information.

Kronick services organizations and individuals across a variety of industries, and in the course of its work on behalf of clients, is sometimes provided access to personal information as a part of the client engagement. Kronick receives and utilizes this data solely to provide legal counsel to its clients.

Kronick was in possession of your information due to its work for [Variable Data Field - Extra 1]. This notice explains the incident and steps we have taken in response, and provides additional information on steps you may take to help protect your information.

What Happened

In August 2024, Kronick discovered unauthorized access to its network from an unknown third party. Once we detected the incident, our team immediately disconnected systems, reset all user passwords, and disabled and reset all service accounts. After learning that the unknown third party claiming responsibility for the incident temporarily posted the data it took from the Kronick network to a website the unknown third party maintains outside the confines of the publicly accessible and indexed Internet, Kronick began an investigation and engaged leading third-party cybersecurity and forensic experts to assist. Kronick also notified law enforcement of the incident. The data is no longer posted on the dark web and, at this time, Kronick has no reason to believe this data was retained by the unknown third party or that any additional data was taken.

The investigation confirmed that the unknown third party gained access to certain Kronick internal systems and obtained data from those systems. A thorough review of the affected data was conducted to identify what information was involved and to identify individuals to whom the data related.

What Information Was Involved

The review determined that the data involved may have contained some of your personal information, including your name, and one or more of the following: Social Security Number, date of birth, driver's license number, medical information, and health insurance information.

What We Are Doing

To help prevent a similar type of incident from occurring in the future, Kronick implemented additional security protocols designed to enhance the security of its network, internal systems, and applications. Kronick will also continue to evaluate additional steps that may be taken to further increase its defenses. In addition, Kronick is continuing to support federal law enforcement's investigation into the incident.

What You Can Do

While Kronick is not aware of any evidence that your personal information has been misused, we wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. We encourage you to remain vigilant about protecting your personal information and, as a precaution, **Kronick is offering you complimentary access to Experian credit monitoring for 24 months**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This complimentary access is being offered to you by Kronick completely free for 24 months and enrolling in this program will not hurt your credit score.

For more information on Experian, including instructions on how to activate your complimentary 24-month membership, as well as other steps you may take to help protect your personal information, please see the additional information provided in the following pages.

For More Information

Kronick takes the security of your personal information seriously and sincerely regrets that this incident occurred. For more information, or if you have any questions, please call 833-931-7699, Monday through Friday, between 6:00 a.m. and 6:00 p.m. Pacific Time. If you have a speech or hearing impairment and use a TTY, call 711.

Sincerely,

KRONICK, MOSKOVITZ, TIEDEMANN & GIRARD
A Professional Corporation

Experian Enrollment Information

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **August 29, 2025** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-7699 by August 29, 2025. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian files for indicators of fraud.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-931-7699. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:
You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.
It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag.

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743- 0023**.**

For New York Residents: You may contact the New York Department of State Division of Consumer Protection*,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General*,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Texas residents: You may contact and obtain information from your state attorney general at: Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identity-theft or contact the Identity Theft Hotline at 800-621-0508 (toll-free).

Reporting of identity theft and obtaining a police report.
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.