KIRKLAND & ELLIS LLP

333 West Wolf Point Plaza
Chicago, IL 60654
United States

Sunil Shenoi
To Call Writer Directly:
+1 312 862 3028
sunil.shenoi@kirkland.com

+1 312 862 2000

Facsimile:
+1 312 862 2200

www.kirkland.com

July 21, 2026

VIA PORTAL SUBMISSION

Washington State Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

To Whom It May Concern:

In accordance with RCWA 19.255.010, I am writing on behalf of Unlimited Technology Systems, LLC ("Unlimited") to notify you of a recent data security incident. Unlimited provides practice management software to various health care organizations and providers.

On October 19, 2025, Unlimited discovered unauthorized activity within its commercial datacenter. Upon discovering the unauthorized activity, Unlimited hired a leading cybersecurity forensic firm to conduct an investigation, notified law enforcement, and conducted a review of the data involved. Through this investigation, Unlimited found evidence that an unauthorized actor obtained a copy of some individuals' personal information between October 5 and October 10, 2025.

Some of the data involved in the security incident may have included individuals' name and information in one or more of the following categories: health insurance and patient balance information (such as insurance policy numbers or claims/benefits information), medical information (such as medical record number, dates of service, and diagnosis information), scanned documents (such as driver's licenses or other government identification, insurance cards, and intake forms), Social Security number, and other personal information (such as date of birth, email, address, phone number, or demographic information). The particular type of information involved depends on the individual.

The data involved in the incident does not include full patient medical records, medical imaging, or financial information, such as credit card or bank account information.

Since discovering the security incident, Unlimited has implemented enhanced security measures to prevent similar incidents from occurring in the future. Unlimited has worked diligently with impacted data owners to identify mailing addresses for individuals whose personal information may have been involved, and offered to notify the relevant individuals. Unlimited began providing notice of this incident on behalf and at the request of impacted data owners on approximately July 21, 2026. Unlimited will notify approximately 724 applicable Washington residents via United States Postal Service mail. Notifications are being sent on a rolling basis, and Unlimited will update this notice as needed. In addition, Unlimited is offering 24 months of identity monitoring services at no cost to notified individuals. Attached as **Exhibit A** is a sample of the notice to be sent to individuals in your state.

Please do not hesitate to contact me if you have any questions.

Sincerely,

Sunil Shenoi

UNLIMITED

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

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

Notice of Data Breach

Dear <<First_name>> <<Last_name>>,

You are receiving this letter because your information was involved in an October 2025 data security incident at Unlimited Technology Systems, LLC ("Unlimited"), which provides practice management software to various health care organizations and providers. While we are unaware of any attempted or actual misuse of any information involved in this incident, we are providing you with an overview of the data security incident, our response to it, the support we are offering to you, and additional measures you can take to help protect your personal information, should you find it necessary.

What Happened

On October 19, 2025, we discovered unauthorized activity within our commercial datacenter. Upon discovering the unauthorized activity, Unlimited hired a leading cybersecurity forensic firm to conduct an investigation, notified law enforcement, and conducted a review of the data involved. Through this investigation, we found evidence that an unauthorized actor obtained a copy of some of your personal information between October 5 and October 10, 2025.

What Information Was Involved

Unlimited has determined that some of the data involved in the security incident may have included your name and information in one or more of the following categories: health insurance and patient balance information (such as insurance policy numbers or claims/benefits information), medical information (such as medical record number, dates of service, and diagnosis information), scanned documents (such as driver's licenses or other government identification, insurance cards, and intake forms), Social Security number, and other personal information (such as date of birth, email, address, phone number, or demographic information). The particular type of information involved depends on the individual.

The data involved in the incident does not include full patient medical records, medical imaging, or financial information, such as credit card or bank account information.

What We Are Doing

We implemented enhanced security measures to prevent similar incidents from occurring in the future. Additionally, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

<u>How to Activate Your Identity Monitoring Services:</u>

1. You must activate your identity monitoring services by **<<b2b_text_6 (Activation Deadline)>>**. Your Activation Code will not work after this date.
2. Visit **<u>Enroll.krollmonitoring.com/redeem</u>** to activate your identity monitoring services.
3. Provide Your Activation Code: **<<b2b_text_5 (Activation Code)>>** and Your Verification ID: **<<b2b_text_4 (Verification ID)>>**

Additional information describing the offered services is also included with this letter.

For More Information

If you have questions, please call (844) 576-3063**,** Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for any unauthorized or suspicious activity. Any such activities should be reported to your financial institutions immediately. You may also review the enclosure that follows this letter for general guidance on how to protect your personal information.

Unlimited takes this matter seriously and is committed to protecting the privacy and security of the information entrusted to us. We deeply regret any inconvenience caused by this incident and will continue to improve our system security to better support our customers, and in turn, their patients.

Sincerely,

Unlimited Technology Systems, LLC

Reference Guide

Take Advantage of Your Identity Monitoring Services. You have been provided with access to the following services from Kroll:

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

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assisting 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.

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.

Order Your Free Credit Report. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

Monitoring. You should always remain vigilant for incidents of fraud and identity theft by reviewing bank and payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately reporting any suspicious activity or incidents of identity theft. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft/.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. You can place fraud alerts with the three credit bureaus by phone, by mail, or online (see below). The bureau you contact will notify the other two bureaus about the fraud alert. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
1-888-378-4329

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/fraud/center.html
1-888-397-3742

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-victim-resource/place-fraud-alert
1-800-916-8800

Consider Placing a Security Freeze on Your Credit File. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*.

To place a security freeze on your credit report, you must make a request to each consumer reporting agency by phone, by mail, or online (see below). The consumer reporting agencies may require proper identification prior to honoring your request, so to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-888-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. This office can be reached at: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, www.marylandattorneygeneral.gov.

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze (at no charge) as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. This office can be reached at: Office of the Attorney General, The Capital, Albany, NY 12224-0341, (800) 771-7755, www.ag.ny.gov.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. This office can be reached at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov.

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General. This office can be reached at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General. This office can be reached at: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov.

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia. This office can be reached at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, www.oag.dc.gov.