



N7155-L01-0000001 P001 T00001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 ADULTS
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789
|||

Dear Sample A. Sample:

DaVita Inc. ("DaVita") is writing to share with you some important information regarding a recent incident potentially involving your personal information.

What Happened? On April 12, 2025, we discovered that we experienced a security incident that resulted in unauthorized access to certain DaVita network servers, primarily at its laboratories. Upon discovery, we initiated our incident response protocols and were able to eradicate the unauthorized party from our systems on that day. We also engaged third-party forensic experts to conduct a review of the impacted servers and to assist with containment, eradication of the threat actor, and remediation. We have also reported the incident to law enforcement and continue to cooperate with them in their investigation. Our teams have worked diligently alongside experts to determine what information was accessed and removed by the threat actor. Through an extensive investigation, we understand that the cyber incident started on March 24, 2025, and continued until the threat actor was blocked from our servers on April 12, 2025.

What Information Was Involved? The data involved included information from our dialysis labs database, and on or about June 18, 2025, we were able to determine that your personal information was potentially involved. The involved information varied by individual, and may have included certain demographic information, such as name, address, date of birth, social security number, health insurance-related information, and other identifiers internal to DaVita, as well as certain clinical information, such as health condition, other treatment information, and certain dialysis lab test results. For some individuals, the information included tax identification numbers, and in limited cases images of checks written to DaVita.

What We Are Doing. Upon discovering the incident, we have taken additional steps to safeguard our systems and information by deploying additional security monitoring tools and enhanced system controls.

What You Can Do. To date, there is no evidence that your information has been subject to fraud. Nevertheless, it is advisable to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free annual credit reports for suspicious activity and to detect errors. The enclosed “General Information About Identity Theft Protection” section provides additional information about what you can do.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks® for ## months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute

Para ver el contenido de esta carta de notificación en español, visite www.davita.com/cyberincident.

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 Identity Restoration is available to you for ## months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** November 28, 2025 by 11:59 pm UTC (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 that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by November 28, 2025 at 833-931-7489 Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-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 file 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.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

We sincerely regret that this incident occurred and assure you that protecting the privacy of your information is one of our highest priorities. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-931-7489 toll-free Monday through Friday from 8 am to 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

Sincerely,

DaVita Inc.
Privacy Office

*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.

Para ver el contenido de esta carta de notificación en español, visite www.davita.com/cyberincident.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

Monitor Your Accounts and Credit Reports

To date, there is no evidence that your information has been subject to fraud. Nevertheless, it is always advisable to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-866-349-5191
www.equifax.com

Experian®
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Consider Placing a Fraud Alert

You have the right to place an initial or extended fraud alert on your file at no cost. A fraud alert notifies potential lenders to verify your identification before extending credit in your name. Should you wish to place a fraud alert, please contact any of the agencies listed below.

Equifax®
P.O. Box 1050698
Atlanta, GA 30348-5069
1-800-525-6285
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Experian®
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/help/fraud-alert/

TransUnion®
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Credit Freeze for Credit Reporting Agencies

You also have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. It is free to place, lift or remove a security freeze. You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

Equifax®
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-378-4329
www.equifax.com/personal/credit-report-services

Experian®
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/help/credit-freeze/

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

To request a security freeze, you may need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth

Para ver el contenido de esta carta de notificación en español, visite www.davita.com/cyberincident.



- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

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/documents/bcfc_consumer-rights-summary_2018-09.pdf or www.ftc.gov.

Steps You Can Take if You Are a Victim of Identity Theft

File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

Further information can be obtained from the FTC about steps to take to avoid identity theft at: <http://www.ftc.gov/idtheft>; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State Specific Information

California Residents may visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia residents may contact the District of Columbia Attorney General at 400 6th Street, NW, Washington, D.C. 20001; 1-202-727-3400; and <https://oag.dc.gov/>.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling 1-515-281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky Residents may contact the Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Para ver el contenido de esta carta de notificación en español, visite www.davita.com/cyberincident.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <https://www.marylandattorneygeneral.gov/pages/identitytheft/default.aspx>, calling the Identity Theft Unit at (410) 576-6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with 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 its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

New York residents can learn more about security breach response and identity theft prevention and protection from the New York State Department of State Division of Consumer Protection, by visiting their web site at <https://dos.ny.gov/protecting-yourself-identity-theft> or by contacting federal agencies using the contact information listed above.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <https://ncdoj.gov/protecting-consumers/identity-theft/>, calling 1-919-716-6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling 1-503-378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that 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. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 401-274-4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.

Para ver el contenido de esta carta de notificación en español, visite www.davita.com/cyberincident.

