



400904749999999999

**Must be postmarked or
submitted online
NO LATER THAN
January 19, 2027**

DaVita Ransomware Settlement
Settlement Administrator
P.O. Box 2943
Portland, OR 97208-2943
DVACyberattackSettlement.com

DaVita Ransomware Settlement Claim Form
Jenkins v. DaVita Inc., Case No. 1:25-cv-01358 (D. Colo.)

GENERAL INFORMATION

If your Personal Information was potentially accessed without authorization in the Ransomware Attack involving DaVita, Inc. in April 2025, you may be entitled to benefits from a Settlement.

You may submit a Claim Form for Settlement benefits, outlined below, by visiting the Settlement Website at **DVACyberattackSettlement.com**. Claim Forms must be submitted or postmarked by **January 19, 2027**. If you would prefer to submit by mail, please use the return address at the top of this form.

SETTLEMENT BENEFITS – WHAT YOU MAY GET

You may submit a claim for one or more of these benefits:

(1) Pro Rata Cash Payment:

You may elect to receive a Pro Rata Cash Payment. The payments shall be calculated by dividing remaining funds in the \$10,000,000 Settlement Fund, after payment of Notice and Claims Administration Costs, Attorneys' Fees, Costs, and Expenses Award, Service Awards, and the cost of claimed Credit Monitoring, by the number of eligible claims for Pro Rata Cash Payments. The Pro Rata Cash Payments will be adjusted upwards or downwards based upon the number of valid claims filed.

(2) Credit Monitoring:

In addition to selecting any other Settlement Benefits, you may claim three (3) years of Credit Monitoring that will provide the following benefits: one-bureau Credit Monitoring, dark web monitoring, identity theft insurance coverage for up to \$1,000,000, and fully managed identity recovery services.

(3) Reimbursement for Documented Out-of-Pocket Losses:

All Settlement Class Members who timely submit a valid claim are eligible for reimbursement of up to a total of \$2,500 per person for actual, documented, unreimbursed monetary losses fairly traceable to the Ransomware Attack incurred by a Settlement Class Member between April 11, 2025, and January 19, 2027.

Documented Out-of-Pocket Losses for which reimbursement is available may include, without limitation, actual, documented, unreimbursed costs, expenses, losses, or charges incurred as a result of identity theft, fraud, falsified tax returns, real estate title fraud, financial fraud, government benefits fraud, or other misuse of the Settlement Class Member's Personal Information that is fairly traceable to the Ransomware Attack.

You must submit documentation supporting your Claim Form for Documented Out-of-Pocket Losses. Documentation supporting your losses can include receipts or other documentation not "self-prepared" by you. "Self-prepared" documents such as handwritten receipts are, by themselves, insufficient to qualify for reimbursement for Documented Out-of-Pocket Losses.

Your claim for Pro Rata Cash or Documented Out-of-Pocket Losses may be subject to a pro rata (a legal term meaning equal share) decrease depending upon the total value of timely and valid Claim Forms.

* * *

Please Note: The Settlement Administrator may contact you to request additional documents to process your Claim Form.

For more information and complete instructions, visit **DVACyberattackSettlement.com**.

Please note that Settlement benefits will be distributed after the Settlement is approved by the Court and becomes Final. This may take some time – please be patient.

Questions? Go to **DVACyberattackSettlement.com** or call **1-877-239-8791**

Contact Information

1. NAME (REQUIRED):

First Name

[illegible]

MI

1

Last Name

[illegible]

2. MAILING ADDRESS (REQUIRED):

Street Address

[illegible]

Apt. No.

[illegible]

City

[illegible]

State

--	--

ZIP Code

--	--	--	--	--

3. PHONE NUMBER:

4. EMAIL ADDRESS:

[illegible]

5. UNIQUE ID:

[illegible]

Pro Rata Cash Payment:

☐

I wish to receive a Pro Rata Cash Payment, currently estimated to be \$50.



400904749999999999

Documented Out-of-Pocket Losses

You may submit a Claim Form and provide documentation for reimbursement of up to \$2,500 of Documented Out-of-Pocket Losses per Settlement Class Member.

It is important for you to send reasonable documents that show what happened and how much you lost or spent so that you can be reimbursed.

Documentation supporting your losses can include receipts or other documentation not “self prepared” by you. “Self-prepared” documents such as handwritten receipts are, by themselves, insufficient to receive reimbursement, but can be considered to add clarity to or support other submitted documentation.

To look up more details about how the reimbursement of Documented Out-of-Pocket Losses works, visit **DVACyberattackSettlement.com** or call toll-free **1-877-239-8791**. Please also review the Settlement Agreement on the Settlement Website, which provides more details on the types of expenses that can be claimed. *By filling out the boxes below, you are certifying under penalty of perjury that the money you spent doesn't relate to other ransomware attacks or data breaches; that the expenses detailed below are fairly traceable to the Ransomware Attack to the best of your knowledge, information, and belief; that the expenses detailed below were incurred between April 11, 2025 and the date of this Claim Form; that you have not been reimbursed from any other source for the expenses detailed below; and that you made reasonable efforts to avoid the losses detailed below or to seek reimbursement for the same, including, but not limited to, disputing unauthorized transactions and exhausting all existing credit monitoring insurance and identity theft insurance.*

Expense Type and Examples of Documents	Amount and Date	Description of Expense or Money Spent and Supporting Documents (Identify what you are attaching, and why it's related to the Ransomware Attack)
Professional fees incurred to address identity theft or fraud, such as falsified tax returns, account fraud, and/or identity theft. <i>Examples: Receipts, notices, or account statements reflecting payment for a credit freeze</i>	\$. Date: - - MM DD YYYY	
Other losses or costs resulting from identity theft or fraud (provide detailed description) fairly traceable to the Ransomware Attack. <i>Examples: Account statement with unauthorized charges circled; bank fees, and fees for credit reports, credit monitoring, or other identity theft insurance products purchased</i>	\$. Date: - - MM DD YYYY	
Other expenses such as notary, fax, postage, copying, mileage, long-distance telephone charges, or professional fees related to the Ransomware Attack. <i>Examples: Phone bills, receipts, detailed list of addresses you traveled to (e.g., police station, IRS office), reason why you traveled there (e.g., police report or letter from IRS re: falsified tax return) and number of miles you traveled</i>	\$. Date: - - MM DD YYYY	

Questions? Go to **DVACyberattackSettlement.com** or call **1-877-239-8791**

You may choose to elect to receive three (3) years of free one-bureau Credit Monitoring.

Please fill out **ONLY ONE** of the payment options below.

Page 4