Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6706
Joshua.Mooney@kennedyslaw.com
April 6, 2026

By Online Submission

Attorney General Nick Brown
Office of Attorney General
1125 Washington St. SE
P.O. Box 40100
Olympia, WA 98504

Re: Notice of Data Incident

Dear Attorney General Nick Brown:

We write on behalf of our client Rainier Clinical Research Center to notify your office of a data breach pursuant to RCW § 19.255.010. Rainier is clinical healthcare research facility located in Renton, Washington. The incident in question involved the personal identifiable information of 650 residents in the State of Washington.

On January 18, 2026, Rainier learned of unauthorized activity in their system resulting from a data security incident suffered by their IT managed service provider. Upon discovery, they took immediate action to launch an investigation to address the incident and terminate further unauthorized access. They retained our office, and we engaged the cyber security forensics firm CFC Security, Inc. d/b/a/ CFC Response, and notified federal law enforcement. After an investigation, they determined that an unauthorized actor gained access to their systems between January 15-18, 2026, and that information potentially acquired involved individual's PII. Specifically, the PII involved includes individuals' first name or initial with last name and Social Security number. For two (2) Washington residents, their Driver's License number also was involved.

Rainier notified these individuals via First Class U.S. mail on April 6, 2026. Rainier is offering 12 months of single bureau credit monitoring, fraud consultation, and identity theft restoration services through Kroll to individuals included in the data set. Rainier has set up a professional call center to respond to individuals' inquiries and to assist with fraud consultation resources and credit monitoring enrollment. Sample copies of the notification letters are enclosed. Rainier is also reviewing its existing security policies and protections previously in

place on its network and adopting additional security to safeguard against evolving threats moving forward. Notification will also be made concurrently to the Montana Office of Attorney General due to one (1) individual's residential address location.

Should you have any further questions at this stage, please do not hesitate to contact me. Thank you.

Very truly yours,

/s/Joshua A. Mooney

Joshua A. Mooney

Partner
for Kennedys

Enclosures: Sample Consumer Notification Letters (2)

RAINIER CLINICAL
RESEARCH CENTER, LLC

Phone 425.251.1720 | Fax 425.251.1723
800 SW 39th Street, Suite 110 | Renton, WA 98057

www.rainier-research.com

<<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>>

KROLL
SCAN TO ENROLL

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

Re: ***Notice of Data Event***

Dear <<First_name>> <<Last_name>>:

Rainier Clinical Research Center writes to inform you of a data security incident that may have involved your personally identifiable information ("PII"). This notice explains the incident, the steps we have taken in response, and steps that individuals can take for further protection.

What Happened? On January 18, 2026, we learned of unauthorized activity in our system resulting from a data security incident suffered by our IT managed service provider. Upon discovery, we took immediate action to launch an investigation to address the incident and terminate further unauthorized access. We also retained leading cyber security experts and notified law enforcement. After an investigation, we determined that an unauthorized actor gained access to our systems between January 15-18, 2026, and that information potentially acquired involved your PII, as described below.

What Information Was Involved? The PII involved was your first name or initial with last name and Social Security number and Driver's License Number.

What We Are Doing. After becoming aware of this incident, we took immediate additional safeguards to protect our network and engaged cybersecurity specialists to conduct a thorough investigation. We also have notified the Washington Office of Attorney General. In addition, as an added protection, we are offering the opportunity to enroll in 12 months of identity monitoring services through Kroll, a company that specializes in consumer protection. Instructions for how to enroll are enclosed.

What You Can Do. We have no information to suggest that your PII has been or will be used to engage in identify theft. Nor is the fact that you are receiving this letter an indication that you will be a victim of fraud. But as a general matter, it is prudent to remain vigilant of identity theft. You should review and monitor your account statements and credit reports for suspicious activity, and report any such activity to the appropriate financial institution or provider. You also may enroll in the credit monitoring and identity theft services being offered.

For More Information. We regret that this incident occurred or any inconvenience it may cause. If you have questions, you may call our professional toll-free call center at (844) 403-4526 Monday through Friday, excluding major U.S. holidays, between 9 a.m. and 6:30 p.m. Eastern Standard Time.

Sincerely,

Rainier Clinical Research Center

Enclosure: *Steps You Can Take To Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Information

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Credit Freeze Instructions: As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion
1-800-680-7289
www.transunion.com

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094

Experian
1-888-397-3742
www.experian.com

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013

Experian Credit Freeze
P.O. Box 9554
Allen, TX 75013

Equifax
1-888-298-0045
www.equifax.com

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Additional Information

This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.A complaint may be filed with the FTC online at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides information about fraud alerts and security freezes.

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, or https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico Residents, the New Mexico Attorney General may be contacted at the New Mexico Department of Justice, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501; (505) 490-4060; or https://nmdoj.gov/.

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; or www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Justice Building, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; or https://www.doj.state.or.us/.

For *Rhode Island residents*, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or www.riag.ri.gov. The number of Rhode Island residents whose information was involved in this incident is none.

You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. or www.ftc.gov.

KROLL

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. 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.

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, assistance 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.

RAINIER CLINICAL RESEARCH CENTER, LLC

Phone 425.251.1720 | Fax 425.251.1723
800 SW 39th Street, Suite 110 | Renton, WA 98057

www.rainier-research.com

<<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)

Re: ***Notice of Data Event***

Dear <<First_name>> <<Last_name>>:

Rainier Clinical Research Center writes to inform you of a data security incident that may have involved your personally identifiable information ("PII"). This notice explains the incident, the steps we have taken in response, and steps that individuals can take for further protection.

What Happened? On January 18, 2026, we learned of unauthorized activity in our system resulting from a data security incident suffered by our IT managed service provider. Upon discovery, we took immediate action to launch an investigation to address the incident and terminate further unauthorized access. We also retained leading cyber security experts and notified law enforcement. After an investigation, we determined that an unauthorized actor gained access to our systems between January 15-18, 2026, and that information potentially acquired involved your PII, as described below.

What Information Was Involved? The PII involved was your first name or initial with last name and Social Security number.

What We Are Doing. After becoming aware of this incident, we took immediate additional safeguards to protect our network and engaged cybersecurity specialists to conduct a thorough investigation. We also have notified the Washington Office of Attorney General. In addition, as an added protection, we are offering the opportunity to enroll in 12 months of identity monitoring services through Kroll, a company that specializes in consumer protection. Instructions for how to enroll are enclosed.

What You Can Do. We have no information to suggest that your PII has been or will be used to engage in identify theft. Nor is the fact that you are receiving this letter an indication that you will be a victim of fraud. But as a general matter, it is prudent to remain vigilant of identity theft. You should review and monitor your account statements and credit reports for suspicious activity, and report any such activity to the appropriate financial institution or provider. You also may enroll in the credit monitoring and identity theft services being offered.

For More Information. We regret that this incident occurred or any inconvenience it may cause. If you have questions, you may call our professional toll-free call center at (844) 403-4526 Monday through Friday, excluding major U.S. holidays, between 9 a.m. and 6:30 p.m. Eastern Standard Time.

Sincerely,

Rainier Clinical Research Center

Enclosure: *Steps You Can Take To Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Information

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Credit Freeze Instructions: As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion
1-800-680-7289
www.transunion.com

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094

Experian
1-888-397-3742
www.experian.com

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013

Experian Credit Freeze
P.O. Box 9554
Allen, TX 75013

Equifax
1-888-298-0045
www.equifax.com

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Additional Information

This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.A complaint may be filed with the FTC online at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides information about fraud alerts and security freezes.

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, or https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico Residents, the New Mexico Attorney General may be contacted at the New Mexico Department of Justice, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501; (505) 490-4060; or https://nmdoj.gov/.

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; or www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Justice Building, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; or https://www.doj.state.or.us/.

For *Rhode Island residents*, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or www.riag.ri.gov. The number of Rhode Island residents whose information was involved in this incident is none.

You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. or www.ftc.gov.

KROLL

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. 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.

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, assistance 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.

Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6706
Joshua.Mooney@kennedyslaw.com
April 6, 2026

By Online Submission

Attorney General Nick Brown
Office of Attorney General
1125 Washington St. SE
P.O. Box 40100
Olympia, WA 98504

Re: Notice of Data Incident

Dear Attorney General Nick Brown:

We write on behalf of our client Rainier Clinical Research Center to notify your office of a data breach pursuant to RCW § 19.255.010. Rainier is clinical healthcare research facility located in Renton, Washington. The incident in question involved the personal identifiable information of 650 residents in the State of Washington.

On January 18, 2026, Rainier learned of unauthorized activity in their system resulting from a data security incident suffered by their IT managed service provider. Upon discovery, they took immediate action to launch an investigation to address the incident and terminate further unauthorized access. They retained our office, and we engaged the cyber security forensics firm CFC Security, Inc. d/b/a/ CFC Response, and notified federal law enforcement. After an investigation, they determined that an unauthorized actor gained access to their systems between January 15-18, 2026, and that information potentially acquired involved individual's PII. Specifically, the PII involved includes individuals' first name or initial with last name and Social Security number. For two (2) Washington residents, their Driver's License number also was involved.

Rainier notified these individuals via First Class U.S. mail on April 6, 2026. Rainier is offering 12 months of single bureau credit monitoring, fraud consultation, and identity theft restoration services through Kroll to individuals included in the data set. Rainier has set up a professional call center to respond to individuals' inquiries and to assist with fraud consultation resources and credit monitoring enrollment. Sample copies of the notification letters are enclosed. Rainier is also reviewing its existing security policies and protections previously in

place on its network and adopting additional security to safeguard against evolving threats moving forward. Notification will also be made concurrently to the Montana Office of Attorney General due to one (1) individual's residential address location.

Should you have any further questions at this stage, please do not hesitate to contact me. Thank you.

Very truly yours,

/s/Joshua A. Mooney

Joshua A. Mooney

Partner
for Kennedys

Enclosures: Sample Consumer Notification Letters (2)

RAINIER CLINICAL
RESEARCH CENTER, LLC

Phone 425.251.1720 | Fax 425.251.1723
800 SW 39th Street, Suite 110 | Renton, WA 98057

www.rainier-research.com

<<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>>

KROLL
SCAN TO ENROLL

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

Re: ***Notice of Data Event***

Dear <<First_name>> <<Last_name>>:

Rainier Clinical Research Center writes to inform you of a data security incident that may have involved your personally identifiable information ("PII"). This notice explains the incident, the steps we have taken in response, and steps that individuals can take for further protection.

What Happened? On January 18, 2026, we learned of unauthorized activity in our system resulting from a data security incident suffered by our IT managed service provider. Upon discovery, we took immediate action to launch an investigation to address the incident and terminate further unauthorized access. We also retained leading cyber security experts and notified law enforcement. After an investigation, we determined that an unauthorized actor gained access to our systems between January 15-18, 2026, and that information potentially acquired involved your PII, as described below.

What Information Was Involved? The PII involved was your first name or initial with last name and Social Security number and Driver's License Number.

What We Are Doing. After becoming aware of this incident, we took immediate additional safeguards to protect our network and engaged cybersecurity specialists to conduct a thorough investigation. We also have notified the Washington Office of Attorney General. In addition, as an added protection, we are offering the opportunity to enroll in 12 months of identity monitoring services through Kroll, a company that specializes in consumer protection. Instructions for how to enroll are enclosed.

What You Can Do. We have no information to suggest that your PII has been or will be used to engage in identify theft. Nor is the fact that you are receiving this letter an indication that you will be a victim of fraud. But as a general matter, it is prudent to remain vigilant of identity theft. You should review and monitor your account statements and credit reports for suspicious activity, and report any such activity to the appropriate financial institution or provider. You also may enroll in the credit monitoring and identity theft services being offered.

For More Information. We regret that this incident occurred or any inconvenience it may cause. If you have questions, you may call our professional toll-free call center at (844) 403-4526 Monday through Friday, excluding major U.S. holidays, between 9 a.m. and 6:30 p.m. Eastern Standard Time.

Sincerely,

Rainier Clinical Research Center

Enclosure: *Steps You Can Take To Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Information

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Credit Freeze Instructions: As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion
1-800-680-7289
www.transunion.com

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094

Experian
1-888-397-3742
www.experian.com

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013

Experian Credit Freeze
P.O. Box 9554
Allen, TX 75013

Equifax
1-888-298-0045
www.equifax.com

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Additional Information

This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.A complaint may be filed with the FTC online at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides information about fraud alerts and security freezes.

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, or https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico Residents, the New Mexico Attorney General may be contacted at the New Mexico Department of Justice, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501; (505) 490-4060; or https://nmdoj.gov/.

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; or www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Justice Building, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; or https://www.doj.state.or.us/.

For *Rhode Island residents*, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or www.riag.ri.gov. The number of Rhode Island residents whose information was involved in this incident is none.

You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. or www.ftc.gov.

KROLL

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. 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.

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, assistance 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.

RAINIER CLINICAL RESEARCH CENTER, LLC

Phone 425.251.1720 | Fax 425.251.1723
800 SW 39th Street, Suite 110 | Renton, WA 98057

www.rainier-research.com

<<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)

Re: ***Notice of Data Event***

Dear <<First_name>> <<Last_name>>:

Rainier Clinical Research Center writes to inform you of a data security incident that may have involved your personally identifiable information ("PII"). This notice explains the incident, the steps we have taken in response, and steps that individuals can take for further protection.

What Happened? On January 18, 2026, we learned of unauthorized activity in our system resulting from a data security incident suffered by our IT managed service provider. Upon discovery, we took immediate action to launch an investigation to address the incident and terminate further unauthorized access. We also retained leading cyber security experts and notified law enforcement. After an investigation, we determined that an unauthorized actor gained access to our systems between January 15-18, 2026, and that information potentially acquired involved your PII, as described below.

What Information Was Involved? The PII involved was your first name or initial with last name and Social Security number.

What We Are Doing. After becoming aware of this incident, we took immediate additional safeguards to protect our network and engaged cybersecurity specialists to conduct a thorough investigation. We also have notified the Washington Office of Attorney General. In addition, as an added protection, we are offering the opportunity to enroll in 12 months of identity monitoring services through Kroll, a company that specializes in consumer protection. Instructions for how to enroll are enclosed.

What You Can Do. We have no information to suggest that your PII has been or will be used to engage in identify theft. Nor is the fact that you are receiving this letter an indication that you will be a victim of fraud. But as a general matter, it is prudent to remain vigilant of identity theft. You should review and monitor your account statements and credit reports for suspicious activity, and report any such activity to the appropriate financial institution or provider. You also may enroll in the credit monitoring and identity theft services being offered.

For More Information. We regret that this incident occurred or any inconvenience it may cause. If you have questions, you may call our professional toll-free call center at (844) 403-4526 Monday through Friday, excluding major U.S. holidays, between 9 a.m. and 6:30 p.m. Eastern Standard Time.

Sincerely,

Rainier Clinical Research Center

Enclosure: *Steps You Can Take To Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Information

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Credit Freeze Instructions: As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion
1-800-680-7289
www.transunion.com

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094

Experian
1-888-397-3742
www.experian.com

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013

Experian Credit Freeze
P.O. Box 9554
Allen, TX 75013

Equifax
1-888-298-0045
www.equifax.com

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Additional Information

This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.A complaint may be filed with the FTC online at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides information about fraud alerts and security freezes.

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, or https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico Residents, the New Mexico Attorney General may be contacted at the New Mexico Department of Justice, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501; (505) 490-4060; or https://nmdoj.gov/.

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; or www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Justice Building, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; or https://www.doj.state.or.us/.

For *Rhode Island residents*, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or www.riag.ri.gov. The number of Rhode Island residents whose information was involved in this incident is none.

You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. or www.ftc.gov.

KROLL

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. 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.

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, assistance 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.