CONSTANGY
Brooks Smith & Prophete

Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
100 Crescent Court, Suite 700
Dallas, TX 75201
LFunk@constangy.com
Mobile: 248.709.9385

August 20, 2026

**VIA ONLINE SUBMISSION**
Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

**Re: Notice of Data Security Incident**

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Spokane United Methodist Homes d/b/a Rockwood Retirement Communities ("Rockwood"), a nonprofit senior living organization headquartered in Spokane, Washington, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Washington's data breach notification statute.

**Nature of the Security Incident**

On or around February 16, 2026, Rockwood became aware of suspicious activity in its network. In response, Rockwood immediately took steps to secure its internal systems and engaged independent forensic experts to investigate what happened and what data might have been affected, if any. As a result of the investigation, Rockwood learned that a limited amount of data may have been acquired without authorization. Rockwood then engaged an independent team to conduct a comprehensive and time-intensive review of those files, and on June 8, 2026, that review determined that certain personal and/or protected health information may have been contained within the affected data. Rockwood has since worked diligently to verify the potentially affected individuals, gather and validate contact information, assess the scope of the impacted information to effectuate notice, and prepare the identity protection services being offered. This process was completed on July 27, 2026.

The information affected varied between individuals but may have included name, Social Security number, driver's license number, payment card number, passport number, financial account information, medical information, health insurance information, and taxpayer identification number. Please note that we have no current evidence to suggest misuse or attempted misuse of personal information involved in the incident to perpetrate identity theft.

**Number of Washington Residents Involved**

On August 20, 2026, Rockwood notified 7,136 Washington residents with available address information of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

**Steps Taken to Address the Incident**

In response to the incident, Rockwood is providing individuals with information about steps that they can take to help protect their personal information and offering eligible individuals complimentary credit monitoring and identity protection services through IDX. This includes 12 months of credit and CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

Additionally, to help reduce the risk of a similar future incident, Rockwood has implemented additional technical security measures throughout the environment. Rockwood has also notified the U.S. Department of Health and Human Services Office for Civil Rights and published notice of the incident on the home page of its website, which will remain for at least ninety (90) days.

**Contact Information**

Rockwood remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at LFunk@Constangy.com.

Sincerely,

Laura K. Funk
Partner, Constangy Cyber Team

Enclosure: Sample Notification Letter

Spokane United Methodist Homes
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

[redacted]

August 20, 2026

Subject: Notice of Data Security Incident

Dear [redacted],

The purpose of this communication is to notify you of a data security incident experienced by Spokane United Methodist Homes d/b/a Rockwood Retirement Communities ("Rockwood") which may have involved your personal information. Rockwood is committed to maintaining the trust of our residents, and the privacy and security of all information in our possession is a top priority. That is why we are notifying you of the event and providing you with resources to help protect your information. We encourage you to read this letter carefully and follow the steps outlined below.

**What Happened?** On or around February 16, 2026, Rockwood became aware of suspicious activity in our network. We immediately took steps to ensure the security of our internal systems and engaged independent forensic experts to investigate what happened and what data might have been affected during the incident, if any. As a result of the investigation, we learned that certain files associated with employees and residents may have been acquired without authorization. We then engaged an independent team to conduct a comprehensive and time-intensive review of those files. On June 8, 2026, that review determined that certain personal information may have been contained within the affected data. We have since worked diligently to verify the potentially affected individuals, gather and validate contact information, and assess the scope of the impacted information to complete this notice. This process was completed on July 27, 2026.

**What Information Was Involved?** We believe that the information involved in this incident may have included your name along with your [redacted]. **Please note that we have no current evidence to suggest misuse of your personal information to perpetuate identity theft.**

**What We Are Doing.** As soon as we discovered this incident, we launched an investigation and took steps to secure our digital environment, which included implementing enhanced security measures to help prevent a similar incident from occurring in the future.

In addition, Rockwood is offering you complimentary credit monitoring and identity protection services. Specifically, these include Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you on the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

**What You Can Do.** Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through TransUnion.

To enroll in Credit Monitoring services at no charge, please go to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted]. Please note that the deadline for enrolling is November 20, 2026. The enrollment requires an internet connection and email account and may not be available to minors under 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**For More Information.** If you have any questions regarding this incident or need assistance, TransUnion representatives are available between 5:00am to 5:00pm Pacific Time, Monday through Friday, excluding major U.S. holidays. If you have any questions, please call 1-866-898-5714. Representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Jim Maxwell
President & CEO
Rockwood Retirement Communities
2903 E 25th Ave.
Spokane, WA 99223

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

| | | |
|---|---|---|
| **Equifax**<br>P.O. Box 105851<br>Atlanta, GA 30348<br>1-800-525-6285<br>www.equifax.com | **Experian**<br>P.O. Box 9532<br>Allen, TX 75013<br>1-888-397-3742<br>www.experian.com | **TransUnion**<br>P.O. Box 2000<br>Chester, PA 19016<br>1-833-799-5355<br>www.transunion.com/<br>get-credit-report |

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

| | | |
|---|---|---|
| **Federal Trade Commission**<br>600 Pennsylvania Ave, NW<br>Washington, DC 20580<br>consumer.ftc.gov<br>877-438-4338 | **Washington Attorney General**<br>1125 Washington Street SE<br>PO Box 40100<br>Olympia, WA 98504<br>atg.wa.gov<br>360-753-6200 | **South Carolina Attorney General**<br>P.O. Box 11549<br>Columbia, S.C. 29211<br>scag.gov<br>1-803-734-3970 |
| **California Attorney General**<br>1300 I Street<br>Sacramento, CA 95814<br>oag.ca.gov/privacy<br>800-952-5225 | **New York Attorney General**<br>The Capitol<br>Albany, NY 12224<br>ag.ny.gov<br>800-771-7755 | **NY Bureau of Internet and Technology**<br>28 Liberty Street<br>New York, NY 10005<br>dos.ny.gov/consumerprotection<br>212.416.8433 |

| | | |
|---|---|---|
| **Maryland Attorney General**<br>St. Paul Plaza<br>200 St. Paul Place<br>Baltimore, MD 21202<br>oag.maryland.gov<br>1-888-743-0023 | **New Mexico Attorney General**<br>408 Galisteo Street, Villagra Building<br>Santa Fe, NM 87501<br>nmdoj.gov/<br>505-490-4060 | **Washington D.C. Attorney General**<br>400 S 6th Street, NW<br>Washington, DC 20001<br>oag.dc.gov/consumer-protection<br>202-442-9828 |
| **Iowa Attorney General**<br>1305 E. Walnut Street<br>Des Moines, Iowa 50319<br>www.iowaattorneygeneral.gov<br>888-777-4590 | **Oregon Attorney General**<br>1162 Court St., NE<br>Salem, OR 97301<br>doj.state.or.us/consumer-protection<br>877-877-9392 | **North Carolina Attorney General**<br>9001 Mail Service Center<br>Raleigh, NC 27699<br>ncdoj.gov/protectingconsumers<br>877-566-7226 |

You also have certain rights under the Fair Credit Reporting Act ("FCRA"): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Spokane United Methodist Homes
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

[redacted]

August 20, 2026



Subject: Notice of Data Security Incident

Dear [redacted],

The purpose of this communication is to notify you of a data security incident experienced by Spokane United Methodist Homes d/b/a Rockwood Retirement Communities ("Rockwood") which may have involved your personal information. Rockwood is committed to maintaining the trust of our residents, and the privacy and security of all information in our possession is a top priority. That is why we are notifying you of the event and providing you with resources to help protect your information. We encourage you to read this letter carefully and follow the steps outlined below.

**What Happened?** On or around February 16, 2026, Rockwood became aware of suspicious activity in our network. We immediately took steps to ensure the security of our internal systems and engaged independent forensic experts to investigate what happened and what data might have been affected during the incident, if any. As a result of the investigation, we learned that certain files associated with employees and residents may have been acquired without authorization. We then engaged an independent team to conduct a comprehensive and time-intensive review of those files. On June 8, 2026, that review determined that certain personal information may have been contained within the affected data. We have since worked diligently to verify the potentially affected individuals, gather and validate contact information, and assess the scope of the impacted information to complete this notice. This process was completed on July 27, 2026.

**What Information Was Involved?** We believe that the information involved in this incident may have included your name along with your [redacted]. **Please note that we have no current evidence to suggest misuse of your personal information to perpetuate identity theft.**

**What We Are Doing.** As soon as we discovered this incident, we launched an investigation and took steps to secure our digital environment, which included implementing enhanced security measures to help prevent a similar incident from occurring in the future.

**What You Can Do.** Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information.

**For More Information.** If you have any questions regarding this incident or need assistance, TransUnion representatives are available between 5:00am to 5:00pm Pacific Time, Monday through Friday, excluding major U.S. holidays. If you have any questions, please call 1-866-898-5714. Representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Jim Maxwell
President & CEO
Rockwood Retirement Communities
2903 E 25th Ave.
Spokane, WA 99223

# STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

| | | |
|---|---|---|
| **Equifax**<br>P.O. Box 105851<br>Atlanta, GA 30348<br>1-800-525-6285<br>www.equifax.com | **Experian**<br>P.O. Box 9532<br>Allen, TX 75013<br>1-888-397-3742<br>www.experian.com | **TransUnion**<br>P.O. Box 2000<br>Chester, PA 19016<br>1-833-799-5355<br>www.transunion.com/<br>get-credit-report |

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

| | | |
|---|---|---|
| **Federal Trade Commission**<br>600 Pennsylvania Ave, NW<br>Washington, DC 20580<br>consumer.ftc.gov<br>877-438-4338 | **Washington Attorney General**<br>1125 Washington Street SE<br>PO Box 40100<br>Olympia, WA 98504<br>atg.wa.gov<br>360-753-6200 | **South Carolina Attorney General**<br>P.O. Box 11549<br>Columbia, S.C. 29211<br>scag.gov<br>1-803-734-3970 |
| **California Attorney General**<br>1300 I Street<br>Sacramento, CA 95814<br>oag.ca.gov/privacy<br>800-952-5225 | **New York Attorney General**<br>The Capitol<br>Albany, NY 12224<br>ag.ny.gov<br>800-771-7755 | **NY Bureau of Internet and Technology**<br>28 Liberty Street<br>New York, NY 10005<br>dos.ny.gov/consumerprotection<br>212.416.8433 |

| | | |
|---|---|---|
| **Maryland Attorney General**<br>St. Paul Plaza<br>200 St. Paul Place<br>Baltimore, MD 21202<br>oag.maryland.gov<br>1-888-743-0023 | **New Mexico Attorney General**<br>408 Galisteo Street, Villagra Building<br>Santa Fe, NM 87501<br>nmdoj.gov/<br>505-490-4060 | **Washington D.C. Attorney General**<br>400 S 6th Street, NW<br>Washington, DC 20001<br>oag.dc.gov/consumer-protection<br>202-442-9828 |
| **Iowa Attorney General**<br>1305 E. Walnut Street<br>Des Moines, Iowa 50319<br>www.iowaattorneygeneral.gov<br>888-777-4590 | **Oregon Attorney General**<br>1162 Court St., NE<br>Salem, OR 97301<br>doj.state.or.us/consumer-protection<br>877-877-9392 | **North Carolina Attorney General**<br>9001 Mail Service Center<br>Raleigh, NC 27699<br>ncdoj.gov/protectingconsumers<br>877-566-7226 |

You also have certain rights under the Fair Credit Reporting Act ("FCRA"): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Spokane United Methodist Homes
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

To the Parent or Guardian of
[redacted]

August 20, 2026

Subject: Notice of Data Security Incident

Dear Parent or Guardian of [redacted],

The purpose of this communication is to notify you of a data security incident experienced by Spokane United Methodist Homes d/b/a Rockwood Retirement Communities ("Rockwood") which may have involved your child's personal information. Rockwood is committed to maintaining the trust of our residents, and the privacy and security of all information in our possession is a top priority. That is why we are notifying you of the event and providing you with resources to help protect your child's information. We encourage you to read this letter carefully and follow the steps outlined below.

**What Happened?** On or around February 16, 2026, Rockwood became aware of suspicious activity in our network. We immediately took steps to ensure the security of our internal systems and engaged independent forensic experts to investigate what happened and what data might have been affected during the incident, if any. As a result of the investigation, we learned that certain files associated with employees and residents may have been acquired without authorization. We then engaged an independent team to conduct a comprehensive and time-intensive review of those files. On June 8, 2026, that review determined that certain personal information may have been contained within the affected data. We have since worked diligently to verify the potentially affected individuals, gather and validate contact information, and assess the scope of the impacted information to complete this notice. This process was completed on July 27, 2026.

**What Information Was Involved?** We believe that the information involved in this incident may have included your child's name along with your child's [redacted]. **Please note that we have no current evidence to suggest misuse of your child's personal information to perpetuate identity theft.**

**What We Are Doing.** As soon as we discovered this incident, we launched an investigation and took steps to secure our digital environment, which included implementing enhanced security measures to help prevent a similar incident from occurring in the future.

In addition, Rockwood is offering complimentary access to Cyber Monitoring services for you and your minor child for 12 months at no charge. Specifically, Cyber monitoring will look out for your and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

**What You Can Do.** Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your child's information. In addition, we encourage you to enroll your child in the identity theft protection services we are offering through TransUnion.

To enroll in the services at no charge, please go to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted]. Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. Please note that the deadline for enrolling is November 20, 2026. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**For More Information.** If you have any questions regarding this incident, TransUnion representatives are available between 5:00am to 5:00pm Pacific Time, Monday through Friday, excluding major U.S. holidays. If you have any questions, please call 1-866-898-5714. Representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your child's information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Jim Maxwell
President & CEO
Rockwood Retirement Communities
2903 E 25th Ave.
Spokane, WA 99223

## Steps You Can Take to Help Protect Your Child's Information

**Review Any Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant and review statements from your child's accounts closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

**Personal Information of a Minor:** You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies is below.

**Security Freeze:** You may place a free credit freeze for minors under age 16. By placing a security freeze, someone who fraudulently acquires the minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, the minor will not be able to borrow money, obtain instant credit, or get a new credit card until the freeze is temporarily lifted or permanently removed. You must separately place a security freeze on the minor's credit file with each credit reporting agency. There is no charge to place, lift, or remove a security freeze on the minor's credit files. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you and/or the minor, including birth or adoption certificate, Social Security card, and government issued identification card. For TransUnion: www.transunion.com/credit-freeze.

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 105788<br>Atlanta, GA 30348<br>1-888-378-4329<br>www.equifax.com | P.O. Box 9532<br>Allen, TX 75013<br>1-800-831-5614<br>www.experian.com | P.O. Box 2000<br>Chester, PA 19016<br>1-833-799-5355<br>www.transunion.com/<br>get-credit-report |

**Fraud Alert:** You may want to consider placing a fraud alert on the minor's credit report. An initial fraud alert is free and will stay on the minor's credit file for at least one year. The alert informs creditors of possible fraudulent activity within the minor's report and requests that the creditor contact you prior to establishing any accounts in the minor's name. To place a fraud alert, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in the minor's file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

| | | |
|---|---|---|
| **Federal Trade Commission**<br>600 Pennsylvania Ave, NW<br>Washington, DC 20580<br>consumer.ftc.gov<br>877-438-4338 | **Washington Attorney General**<br>1125 Washington Street SE<br>PO Box 40100<br>Olympia, WA 98504<br>atg.wa.gov<br>360-753-6200 | **South Carolina Attorney General**<br>P.O. Box 11549<br>Columbia, S.C. 29211<br>scag.gov<br>1-803-734-3970 |
| **California Attorney General**<br>1300 I Street<br>Sacramento, CA 95814<br>oag.ca.gov/privacy<br>800-952-5225 | **New York Attorney General**<br>The Capitol<br>Albany, NY 12224<br>ag.ny.gov<br>800-771-7755 | **NY Bureau of Internet and Technology**<br>28 Liberty Street<br>New York, NY 10005<br>dos.ny.gov/consumerprotection<br>212.416.8433 |
| **Maryland Attorney General**<br>St. Paul Plaza<br>200 St. Paul Place<br>Baltimore, MD 21202<br>oag.maryland.gov<br>1-888-743-0023 | **New Mexico Attorney General**<br>408 Galisteo Street, Villagra Building<br>Santa Fe, NM 87501<br>nmdoj.gov/<br>505-490-4060 | **Washington D.C. Attorney General**<br>400 S 6th Street, NW<br>Washington, DC 20001<br>oag.dc.gov/consumer-protection<br>202-442-9828 |
| **Iowa Attorney General**<br>1305 E. Walnut Street<br>Des Moines, Iowa 50319<br>www.iowaattorneygeneral.gov<br>888-777-4590 | **Oregon Attorney General**<br>1162 Court St., NE<br>Salem, OR 97301<br>doj.state.or.us/consumer-protection<br>877-877-9392 | **North Carolina Attorney General**<br>9001 Mail Service Center<br>Raleigh, NC 27699<br>ncdoj.gov/protectingconsumers<br>877-566-7226 |

Spokane United Methodist Homes
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

To the Parent or Guardian of
[redacted]

August 20, 2026

Subject: Notice of Data Security Incident

Dear Parent or Guardian of [redacted],

The purpose of this communication is to notify you of a data security incident experienced by Spokane United Methodist Homes d/b/a Rockwood Retirement Communities ("Rockwood") which may have involved your child's personal information. Rockwood is committed to maintaining the trust of our residents, and the privacy and security of all information in our possession is a top priority. That is why we are notifying you of the event and providing you with resources to help protect your child's information. We encourage you to read this letter carefully and follow the steps outlined below.

**What Happened?** On or around February 16, 2026, Rockwood became aware of suspicious activity in our network. We immediately took steps to ensure the security of our internal systems and engaged independent forensic experts to investigate what happened and what data might have been affected during the incident, if any. As a result of the investigation, we learned that certain files associated with employees and residents may have been acquired without authorization. We then engaged an independent team to conduct a comprehensive and time-intensive review of those files. On June 8, 2026, that review determined that certain personal information may have been contained within the affected data. We have since worked diligently to verify the potentially affected individuals, gather and validate contact information, and assess the scope of the impacted information to complete this notice. This process was completed on July 27, 2026.

**What Information Was Involved?** We believe that the information involved in this incident may have included your child's name along with your child's [redacted]. **Please note that we have no current evidence to suggest misuse of your child's personal information to perpetuate identity theft.**

**What We Are Doing.** As soon as we discovered this incident, we launched an investigation and took steps to secure our digital environment, which included implementing enhanced security measures to help prevent a similar incident from occurring in the future.

**What You Can Do.** Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your child's information.

**For More Information.** If you have any questions regarding this incident, TransUnion representatives are available between 5:00am to 5:00pm Pacific Time, Monday through Friday, excluding major U.S. holidays. If you have any questions, please call 1-866-898-5714. Representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your child's information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Jim Maxwell
President & CEO
Rockwood Retirement Communities
2903 E 25th Ave.
Spokane, WA 99223

## Steps You Can Take to Help Protect Your Child's Information

**Review Any Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant and review statements from your child's accounts closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

**Personal Information of a Minor:** You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies is below.

**Security Freeze:** You may place a free credit freeze for minors under age 16. By placing a security freeze, someone who fraudulently acquires the minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, the minor will not be able to borrow money, obtain instant credit, or get a new credit card until the freeze is temporarily lifted or permanently removed. You must separately place a security freeze on the minor's credit file with each credit reporting agency. There is no charge to place, lift, or remove a security freeze on the minor's credit files. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you and/or the minor, including birth or adoption certificate, Social Security card, and government issued identification card. For TransUnion: www.transunion.com/credit-freeze.

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 105788<br>Atlanta, GA 30348<br>1-888-378-4329<br>www.equifax.com | P.O. Box 9532<br>Allen, TX 75013<br>1-800-831-5614<br>www.experian.com | P.O. Box 2000<br>Chester, PA 19016<br>1-833-799-5355<br>www.transunion.com/<br>get-credit-report |

**Fraud Alert:** You may want to consider placing a fraud alert on the minor's credit report. An initial fraud alert is free and will stay on the minor's credit file for at least one year. The alert informs creditors of possible fraudulent activity within the minor's report and requests that the creditor contact you prior to establishing any accounts in the minor's name. To place a fraud alert, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in the minor's file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

| | | |
|---|---|---|
| **Federal Trade Commission**<br>600 Pennsylvania Ave, NW<br>Washington, DC 20580<br>consumer.ftc.gov<br>877-438-4338 | **Washington Attorney General**<br>1125 Washington Street SE<br>PO Box 40100<br>Olympia, WA 98504<br>atg.wa.gov<br>360-753-6200 | **South Carolina Attorney General**<br>P.O. Box 11549<br>Columbia, S.C. 29211<br>scag.gov<br>1-803-734-3970 |
| **California Attorney General**<br>1300 I Street<br>Sacramento, CA 95814<br>oag.ca.gov/privacy<br>800-952-5225 | **New York Attorney General**<br>The Capitol<br>Albany, NY 12224<br>ag.ny.gov<br>800-771-7755 | **NY Bureau of Internet and Technology**<br>28 Liberty Street<br>New York, NY 10005<br>dos.ny.gov/consumerprotection<br>212.416.8433 |
| **Maryland Attorney General**<br>St. Paul Plaza<br>200 St. Paul Place<br>Baltimore, MD 21202<br>oag.maryland.gov<br>1-888-743-0023 | **New Mexico Attorney General**<br>408 Galisteo Street, Villagra Building<br>Santa Fe, NM 87501<br>nmdoj.gov/<br>505-490-4060 | **Washington D.C. Attorney General**<br>400 S 6th Street, NW<br>Washington, DC 20001<br>oag.dc.gov/consumer-protection<br>202-442-9828 |
| **Iowa Attorney General**<br>1305 E. Walnut Street<br>Des Moines, Iowa 50319<br>www.iowaattorneygeneral.gov<br>888-777-4590 | **Oregon Attorney General**<br>1162 Court St., NE<br>Salem, OR 97301<br>doj.state.or.us/consumer-protection<br>877-877-9392 | **North Carolina Attorney General**<br>9001 Mail Service Center<br>Raleigh, NC 27699<br>ncdoj.gov/protectingconsumers<br>877-566-7226 |

Spokane United Methodist Homes
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

[redacted]

August 20, 2026



Subject: Notice of Data Security Incident

Dear [redacted],

The purpose of this communication is to notify you of a data security incident experienced by Spokane United Methodist Homes d/b/a Rockwood Retirement Communities ("Rockwood") which may have involved your personal information. Rockwood is committed to maintaining the trust of our residents, and the privacy and security of all information in our possession is a top priority. That is why we are notifying you of the event and providing you with resources to help protect your information. We encourage you to read this letter carefully and follow the steps outlined below.

**What Happened?** On or around February 16, 2026, Rockwood became aware of suspicious activity in our network. We immediately took steps to ensure the security of our internal systems and engaged independent forensic experts to investigate what happened and what data might have been affected during the incident, if any. As a result of the investigation, we learned that certain files associated with employees and residents may have been acquired without authorization. We then engaged an independent team to conduct a comprehensive and time-intensive review of those files. On June 8, 2026, that review determined that certain personal information may have been contained within the affected data. We have since worked diligently to verify the potentially affected individuals, gather and validate contact information, and assess the scope of the impacted information to complete this notice. This process was completed on July 27, 2026.

**What Information Was Involved?** We believe that the information involved in this incident may have included your name along with your [redacted]. **Please note that we have no current evidence to suggest misuse of your personal information to perpetuate identity theft.**

**What We Are Doing.** As soon as we discovered this incident, we launched an investigation and took steps to secure our digital environment, which included implementing enhanced security measures to help prevent a similar incident from occurring in the future.

In addition, Rockwood is offering you complimentary credit monitoring and identity protection services. Specifically, these include Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you on the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

**What You Can Do.** Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through TransUnion.

To enroll in Credit Monitoring services at no charge, please go to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted]. Please note that the deadline for enrolling is November 20, 2026. The enrollment requires an internet connection and email account and may not be available to minors under 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**For More Information.** If you have any questions regarding this incident or need assistance, TransUnion representatives are available between 5:00am to 5:00pm Pacific Time, Monday through Friday, excluding major U.S. holidays. If you have any questions, please call 1-866-898-5714. Representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Jim Maxwell
President & CEO
Rockwood Retirement Communities
2903 E 25th Ave.
Spokane, WA 99223

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 105851<br>Atlanta, GA 30348<br>1-800-525-6285<br>www.equifax.com | P.O. Box 9532<br>Allen, TX 75013<br>1-888-397-3742<br>www.experian.com | P.O. Box 2000<br>Chester, PA 19016<br>1-833-799-5355<br>www.transunion.com/get-credit-report |

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

| | | |
|---|---|---|
| **Federal Trade Commission**<br>600 Pennsylvania Ave, NW<br>Washington, DC 20580<br>consumer.ftc.gov<br>877-438-4338 | **Washington Attorney General**<br>1125 Washington Street SE<br>PO Box 40100<br>Olympia, WA 98504<br>atg.wa.gov<br>360-753-6200 | **South Carolina Attorney General**<br>P.O. Box 11549<br>Columbia, S.C. 29211<br>scag.gov<br>1-803-734-3970 |
| **California Attorney General**<br>1300 I Street<br>Sacramento, CA 95814<br>oag.ca.gov/privacy<br>800-952-5225 | **New York Attorney General**<br>The Capitol<br>Albany, NY 12224<br>ag.ny.gov<br>800-771-7755 | **NY Bureau of Internet and Technology**<br>28 Liberty Street<br>New York, NY 10005<br>dos.ny.gov/consumerprotection<br>212.416.8433 |

| | | |
|---|---|---|
| **Maryland Attorney General**<br>St. Paul Plaza<br>200 St. Paul Place<br>Baltimore, MD 21202<br>oag.maryland.gov<br>1-888-743-0023 | **New Mexico Attorney General**<br>408 Galisteo Street, Villagra Building<br>Santa Fe, NM 87501<br>nmdoj.gov/<br>505-490-4060 | **Washington D.C. Attorney General**<br>400 S 6th Street, NW<br>Washington, DC 20001<br>oag.dc.gov/consumer-protection<br>202-442-9828 |
| **Iowa Attorney General**<br>1305 E. Walnut Street<br>Des Moines, Iowa 50319<br>www.iowaattorneygeneral.gov<br>888-777-4590 | **Oregon Attorney General**<br>1162 Court St., NE<br>Salem, OR 97301<br>doj.state.or.us/consumer-protection<br>877-877-9392 | **North Carolina Attorney General**<br>9001 Mail Service Center<br>Raleigh, NC 27699<br>ncdoj.gov/protectingconsumers<br>877-566-7226 |

You also have certain rights under the Fair Credit Reporting Act ("FCRA"): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.