



Matthew Toldero, Partner
Cybersecurity & Data Privacy Team
One West 4th Street
Suite 850
Winston-Salem, NC 27101
Email: mtoldero@constangy.com
Phone: 336.448.8552

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

December 11, 2025

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: Morningside Services- Preliminary Notice of Data Event

To Whom It May Concern:

We represent Morningside Services (“Morningside”) located in Olympia Washington, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately 1,534 Washington residents. By providing this notice, Morningside does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On or about June 20, 2025, Morningside became aware of unusual network activity and immediately took steps to secure its systems. Morningside immediately began an investigation. The investigation determined that certain Morningside data may have been acquired without authorization on or about June 20, 2025. Morningside then undertook a comprehensive programmatic and manual review of the potentially affected data. That review completed on November 17, 2025. Morningside identified that certain individual information was potentially affected.

2. Notice to Washington Residents

On or about December 11, 2025, Morningside provided written notice of this incident to approximately 1,534 Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

3. Other Steps Taken and To Be Taken

Upon discovering the event, Morningside moved quickly to investigate and respond to the incident, assess the security of systems, and identify potentially affected individuals. Further, Morningside notified law enforcement regarding the event. Morningside is also working to implement additional safeguards and training to its employees. Morningside is providing access to credit monitoring services for 12 months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Morningside is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Morningside is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 336.448.8552.

Very truly yours,

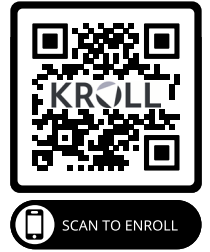
A handwritten signature in black ink that reads "Matthew Toldero". The signature is written in a cursive, flowing style with a large, stylized 'M' and 'T'.

Matthew Toldero, Partner
Constangy, Brooks, Smith & Prophete LLP



<<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>>



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

Subject: Notice of Data Security Incident

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

We are writing to inform you of a data security incident that may have affected your personal information. Morningside takes the privacy and security of all information in our possession very seriously. This letter has information about the incident and steps you can take to protect your information, including enrolling in the complimentary identity monitoring services we are making available to you.

What Happened. On or about November 17, 2025, we learned that personal information of certain individuals was subject to unauthorized access and acquisition. The incident was the result of suspicious activity it first learned of on or about June 20, 2025. Upon discovery, we immediately took steps to secure our systems and engage cybersecurity experts to assist and complete an investigation. The investigation determined that certain Morningside data may have been acquired without authorization. As a result, Morningside undertook a comprehensive review of the potentially affected files with the assistance of an outside vendor, which concluded on September 24, 2025. Our review identified that some of your information may have been involved.

What Information Was Involved. The potentially affected information may have included your <<b2b_text_1 (name, data elements)>>. Please note, we have no evidence of misuse or fraud using your information.

What We Are Doing. As soon as we discovered the incident, we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future.

In addition, we have secured the services of Kroll to provide identity monitoring services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Dark Web 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. Additional information describing your services is included with this letter.

For More Information. If you have questions about this letter or need assistance, please call Kroll at (844) 572-2708. Kroll representatives are available Monday through Friday from 6:00 am – 3:30 pm Pacific Time, excluding major U.S. holidays. Kroll representatives can answer questions or concerns you may have regarding this incident.

We take your trust in us and this matter very seriously.

Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Morningside
809 Legion Way SE
Olympia, WA 98501

Steps You Can Take to Help Protect Your Personal 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

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

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.

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.

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

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
[www.marylandattorneygeneral.gov/
Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
[www.doj.state.or.us/
consumer-protection](http://www.doj.state.or.us/consumer-protection)
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General

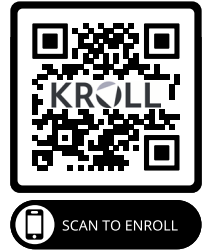
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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.



<<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>>



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

Subject: Notice of Data Security Incident

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

We are writing to inform you of a data security incident that may have affected your personal information. Morningside takes the privacy and security of all information in our possession very seriously. This letter has information about the incident and steps you can take to protect your information, including enrolling in the complimentary identity monitoring services we are making available to you.

What Happened. On or about November 17, 2025, we learned that personal information of certain individuals was subject to unauthorized access and acquisition. The incident was the result of suspicious activity it first learned of on or about June 20, 2025. Upon discovery, we immediately took steps to secure our systems and engage cybersecurity experts to assist and complete an investigation. The investigation determined that certain Morningside data may have been acquired without authorization. As a result, Morningside undertook a comprehensive review of the potentially affected files with the assistance of an outside vendor, which concluded on September 24, 2025. Our review identified that some of your information may have been involved.

What Information Was Involved. The potentially affected information may have included your <<b2b_text_1 (name, data elements)>>. Please note, we have no evidence of misuse or fraud using your information.

What We Are Doing. As soon as we discovered the incident, we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future.

In addition, we have secured the services of Kroll to provide identity monitoring services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Dark Web 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. Additional information describing your services is included with this letter.

For More Information. If you have questions about this letter or need assistance, please call Kroll at (844) 572-2708. Kroll representatives are available Monday through Friday from 6:00 am – 3:30 pm Pacific Time, excluding major U.S. holidays. Kroll representatives can answer questions or concerns you may have regarding this incident.

We take your trust in us and this matter very seriously.

Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Morningside
809 Legion Way SE
Olympia, WA 98501

Steps You Can Take to Help Protect Your Personal 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

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

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.

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.

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

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
[www.marylandattorneygeneral.gov/
Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
[www.doj.state.or.us/
consumer-protection](http://www.doj.state.or.us/consumer-protection)
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
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.