



Melissa J. Sachs
Constangy, Brooks, Smith & Prophete, LLP
msachs@constangy.com
267.219.8332
Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

September 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: Notification of Data Security Incident

Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Union Home Mortgage Corp. (UHM) located at 8241 Dow Circle West, Strongsville, Ohio 44136 in conjunction with their response to a recent data event involving information for Washington residents. The purpose of this letter is to notify you of the incident in accordance with Washington's data breach notification statute. UHM does not waive any rights or defenses under Washington law or personal jurisdiction.

1. Nature of the Security Incident

On June 25, 2025, UHM discovered suspicious activity within its network and immediately initiated an investigation of the matter. It engaged independent cybersecurity experts to assist with the process. As a result of the investigation, we determined that certain files may have been acquired without authorization. By August 26, 2025, the investigation revealed that certain employee and customer files were affected.

2. Number of Affected Washington Residents & Information Involved

The incident involved information for approximately 1,650 Washington residents. The information involved in the incident varied per individual but may have included names and Social Security numbers, home address, dates of birth, loan number, driver's license or government-issued ID numbers, and/or passport numbers.

3. Notification to Affected Individuals

On or about September 11, 2025, UHM provided written notice to Washington residents. Written notice is being provided in substantially the same form as the letter attached herein.

4. Measures Taken to Address the Incident

Upon discovering this incident, UHM moved quickly to investigate and respond to the incident, assess the security of UHM systems, and identify potentially affected individuals. UHM is continuing to review policies and procedures to implement additional measures as appropriate. UHM is also providing access to credit monitoring and identity theft protection services for 12 months through TransUnion to individuals whose personal information was potentially affected by this incident at no cost to these individuals. Finally, UHM has established a toll-free call center to answer questions about the incident and to address related concerns for affected individuals. UHM has also notified appropriate law enforcement and the three main credit reporting agencies.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at msachs@constangy.com or 267.219.8332.

Sincerely,

A handwritten signature in blue ink that reads "Melissa J. Sachs".

Melissa J. Sachs
Partner, Constangy Cyber Team

Encl.: Sample Notification Letter

Union Home Mortgage Corp.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

UNIONHOME
MORTGAGE

September 11, 2025

Re: Notice of Data Security Incident

Dear [REDACTED]

We are writing to inform you of a data security incident that may have affected your personal information. At Union Home Mortgage Corp. (UHM) we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services. We had your information because you were an applicant or co-applicant for a loan or related service we provided directly or indirectly from another originator.

What Happened. On August 26, 2025, UHM learned that your personal information was potentially accessed without authorization. This resulted from an incident we detected on June 25, 2025. At that time we promptly initiated an investigation to determine whether personal information may have been affected and engaged independent digital forensics experts to assist with that process. We also enhanced the security of our environment and informed the FBI. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information involved varied per individual but may have included your name, loan number, Social Security number, driver's license or government-issued ID card number, or date of birth.

What We Are Doing. As soon as UHM discovered the incident, we took the measures described above. We are also offering you complementary credit monitoring and identity protection services for 12 months. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. We recommend that you review and implement the guidance included with this letter about how to protect your information. To enroll in credit monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. 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. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-888-478-3856 Monday through Friday from 8:30 a.m. to 4:30 p.m. Eastern Standard Time. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Union Home Mortgage Corp.
8241 Dow Circle West
Strongsville, Ohio 44136
Tel: 888-478-3856



000010102G0400

P

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. You may also have the right obtain any police report filed about the incident.

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
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
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

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

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



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.

00001020280000

P



Melissa J. Sachs
Constangy, Brooks, Smith & Prophete, LLP
msachs@constangy.com
267.219.8332
Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

September 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: Notification of Data Security Incident

Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Union Home Mortgage Corp. (UHM) located at 8241 Dow Circle West, Strongsville, Ohio 44136 in conjunction with their response to a recent data event involving information for Washington residents. The purpose of this letter is to notify you of the incident in accordance with Washington's data breach notification statute. UHM does not waive any rights or defenses under Washington law or personal jurisdiction.

1. Nature of the Security Incident

On June 25, 2025, UHM discovered suspicious activity within its network and immediately initiated an investigation of the matter. It engaged independent cybersecurity experts to assist with the process. As a result of the investigation, we determined that certain files may have been acquired without authorization. By August 26, 2025, the investigation revealed that certain employee and customer files were affected.

2. Number of Affected Washington Residents & Information Involved

The incident involved information for approximately 1,650 Washington residents. The information involved in the incident varied per individual but may have included names and Social Security numbers, home address, dates of birth, loan number, driver's license or government-issued ID numbers, and/or passport numbers.

3. Notification to Affected Individuals

On or about September 11, 2025, UHM provided written notice to Washington residents. Written notice is being provided in substantially the same form as the letter attached herein.

4. Measures Taken to Address the Incident

Upon discovering this incident, UHM moved quickly to investigate and respond to the incident, assess the security of UHM systems, and identify potentially affected individuals. UHM is continuing to review policies and procedures to implement additional measures as appropriate. UHM is also providing access to credit monitoring and identity theft protection services for 12 months through TransUnion to individuals whose personal information was potentially affected by this incident at no cost to these individuals. Finally, UHM has established a toll-free call center to answer questions about the incident and to address related concerns for affected individuals. UHM has also notified appropriate law enforcement and the three main credit reporting agencies.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at msachs@constangy.com or 267.219.8332.

Sincerely,

A handwritten signature in blue ink that reads "Melissa J. Sachs".

Melissa J. Sachs
Partner, Constangy Cyber Team

Encl.: Sample Notification Letter

Union Home Mortgage Corp.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

UNIONHOME
MORTGAGE

September 11, 2025

Re: Notice of Data Security Incident

Dear [REDACTED]

We are writing to inform you of a data security incident that may have affected your personal information. At Union Home Mortgage Corp. (UHM) we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services. We had your information because you were an applicant or co-applicant for a loan or related service we provided directly or indirectly from another originator.

What Happened. On August 26, 2025, UHM learned that your personal information was potentially accessed without authorization. This resulted from an incident we detected on June 25, 2025. At that time we promptly initiated an investigation to determine whether personal information may have been affected and engaged independent digital forensics experts to assist with that process. We also enhanced the security of our environment and informed the FBI. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information involved varied per individual but may have included your name, loan number, Social Security number, driver's license or government-issued ID card number, or date of birth.

What We Are Doing. As soon as UHM discovered the incident, we took the measures described above. We are also offering you complementary credit monitoring and identity protection services for 12 months. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. We recommend that you review and implement the guidance included with this letter about how to protect your information. To enroll in credit monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. 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. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-888-478-3856 Monday through Friday from 8:30 a.m. to 4:30 p.m. Eastern Standard Time. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Union Home Mortgage Corp.
8241 Dow Circle West
Strongsville, Ohio 44136
Tel: 888-478-3856



000010102G0400

P

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. You may also have the right obtain any police report filed about the incident.

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
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
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

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

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



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.

00001020280000

P

