ALSTON & BIRD

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202-239-3300 | Fax: 202-239-3333

Kimberly Peretti Direct Dial: 202-239-3720 kimberly.peretti@alston.com

March 10, 2026

CONFIDENTIAL
VIA EMAIL

Office of the Washington Attorney General
SecurityBreach@atg.wa.gov

Re: Supplemental Notice of Data Security Incident

To the Office of the Washington Attorney General:

We are writing on behalf of SitusAMC Holdings Corporation ("SitusAMC") to supplement our prior submission to your office dated February 20, 2026 (Submission Number A36744), regarding a data security incident and related notifications to Washington residents.

As previously described, due to the complexity of the underlying data and client relationships, SitusAMC proceeded with individual notifications in advance of final client attribution. The individual notification process has now concluded. All notice letters SitusAMC expects to send to potentially affected individuals on behalf of its clients have been mailed, with the final mailing completed on March 10, 2026.

In total, 20,456 Washington residents have been notified by first-class mail regarding this incident, in accordance with notification requirements under the Gramm-Leach-Bliley Act and applicable state law. A representative copy of the individual notice letters provided to affected Washington residents is enclosed.

At this time, SitusAMC's client attribution process remains ongoing. To the extent any SitusAMC clients subsequently provide direction regarding state Attorney General notifications, SitusAMC will follow up as appropriate with an accounting of those clients and the final number of attributed individuals in your state.

All other details regarding the incident, the categories of information potentially involved, and the remedial measures offered to affected individuals remain as described in SitusAMC's prior submission.

If you have any questions regarding this incident or if you desire further information or assistance, please email me at Kimberly.Peretti@alston.com or call my direct line at (202) 239-3720.

Sincerely,

Kimberly Peretti

Enclosures

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

March 10, 2026

Re: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We are writing to notify you of a recent incident that may have impacted your personal information. SitusAMC Holdings Corporation ("SitusAMC") and/or its subsidiaries and affiliates work with various financial institutions to provide certain mortgage-related services that may involve borrower information and, in some cases, non-borrower information in connection with mortgage transactions. This letter explains the circumstances as we understand them and the resources we are making available to you. At this time, we are not aware of any fraudulent use of your personal information as a result of this incident.

What Happened?
On or about November 12, 2025, SitusAMC became aware of unauthorized access to certain systems within its information technology network. Upon becoming aware of the incident, SitusAMC commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and began taking measures to assess and contain the incident.

The investigation has determined that an unauthorized third party acquired data from certain SitusAMC systems between November 13-21, 2025. As part of the review of the impacted data, SitusAMC identified that some of your personal information may have been involved.

What Information May Have Been Involved?
Based on our investigation, the personal information involved may have included your name, address, date of birth, <<Variable Text 1>> driver's license number or other government-issued identifier, and/or financial account information (such as bank account number or credit or debit card number). <<Variable Text 2>> Not all data elements were involved for each individual.

What We Are Doing
Upon learning of the incident, we commenced an investigation into the nature and scope of the incident and notified law enforcement. We also took measures to further harden and enhance our security.

What You Can Do
We recommend that you remain vigilant for fraud and identity theft. To help address concerns you may have about this incident, we are offering identity theft protection services through IDX, the data breach and recovery services expert.

IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. To activate these services, please take the following steps:

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code: <<ENROLLMENT>>. Please note the deadline to enroll is June 10, 2026.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at (844) 814-3163 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

We encourage you to review and monitor your accounts for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and immediately report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information
If you have questions about this matter or would like additional information, please call toll-free (844) 814-3163, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time (excluding major bank holidays). You may also email us at SitusAMC@idx.us or write to us at 5065 Westheimer Rd., Suite 700E, Houston, TX 77056, Attention: Legal/Regulatory Office. To help our care team respond promptly, please include your full name, a phone number where you can be reached, and a brief description of your question or the assistance you are requesting.

Sincerely,

SitusAMC

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some steps you may consider:

Reviewing Your Accounts and Credit Reports
Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements and periodically obtain your credit report from each of the three national credit reporting companies. Those companies are:

Equifax P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 Equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 Experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 Transunion.com

Under federal law, you are entitled to obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert
A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report
A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will require you to create or provide you with a credential (such as a PIN number or a password) when you place a security freeze. You will need that credential to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft
If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and report suspected incidents of identity theft online at www.IdentityTheft.gov. You can also file a report by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, fraudulent, or unverifiable information. You can find more information about your rights under the FCRA online at https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Additional guidance on how to help protect yourself against possible identity theft is available at https://www.usa.gov/identity-theft.

Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at https://oag.dc.gov/, calling (202) 727-3400, or requesting more information via email oag@dc.gov or mail 400 6th Street NW, Washington DC 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at https://oag.maryland.gov/Pages/oag.aspx, calling the Identity Theft Unit at (410) 576-6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above, and you have rights under the Fair Credit Reporting Act as described above.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the New York State Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: (800) 771-7755.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website at https://ncdoj.gov/protecting-consumers/protecting-your-identity/, calling (919) 716-6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (877) 877-9392 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at (401) 274-4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at https://ago.vermont.gov/.

P.O. Box 989728
West Sacramento, CA 95798-9728

Parent or Legal Guardian of:
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

March 4, 2026

Re: NOTICE OF DATA BREACH

To the Parent or Legal Guardian of <<First Name>> <<Last Name>>:

We are writing to notify you of a recent incident that may have impacted your child's personal information. SitusAMC Holdings Corporation ("SitusAMC") and/or its subsidiaries and affiliates work with various financial institutions to provide certain mortgage-related services that may involve borrower information and, in some cases, non-borrower information in connection with mortgage transactions. This letter explains the circumstances as we understand them and the resources we are making available to your child. At this time, we are not aware of any fraudulent use of your child's personal information as a result of this incident.

What Happened?
On or about November 12, 2025, SitusAMC became aware of unauthorized access to certain systems within its information technology network. Upon becoming aware of the incident, SitusAMC commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and began taking measures to assess and contain the incident.

The investigation has determined that an unauthorized third party acquired data from certain SitusAMC systems between November 13-21, 2025. As part of the review of the impacted data, SitusAMC identified that some of your child's personal information may have been involved.

What Information May Have Been Involved?
Based on our investigation, the personal information involved may have included your child's name, address, date of birth, and Social Security number or individual taxpayer identification number. <<Variable Text 1>>

What We Are Doing
Upon learning of the incident, we commenced an investigation into the nature and scope of the incident and notified law enforcement. We also took measures to further harden and enhance our security.

What You Can Do
We recommend that you remain vigilant for fraud and identity theft. To help address concerns you may have about this incident, we are offering identity protection services for your child through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised. To activate these services, please take the following steps:

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your child's Enrollment Code: <<ENROLLMENT>>. Please note the deadline to enroll is June 4, 2026.

Telephone. Contact IDX at (844) 814-3163 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's credit identity.

We encourage you to review and monitor account statements for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and immediately report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect your child against fraud and identity theft.

For More Information

If you have questions about this matter or would like additional information, please call toll-free (844) 814-3163, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time (excluding major bank holidays). You may also email us at SitusAMC@idx.us or write to us at 5065 Westheimer Rd., Suite 700E, Houston, TX 77056, Attention: Legal/Regulatory Office. To help our care team respond promptly, please include your full name and child's name, a phone number where you can be reached, and a brief description of your question or the assistance you are requesting.

Sincerely,

SitusAMC

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some steps you may consider:

Reviewing Your Accounts and Credit Reports
Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements and periodically obtain your credit report from each of the three national credit reporting companies. Those companies are:

Equifax P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 Equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 Experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 Transunion.com

Under federal law, you are entitled to obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert
A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report
A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will require you to create or provide you with a credential (such as a PIN number or a password) when you place a security freeze. You will need that credential to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft
If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and report suspected incidents of identity theft online at www.IdentityTheft.gov. You can also file a report by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, fraudulent, or unverifiable information. You can find more information about your rights under the FCRA online at https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Additional guidance on how to help protect yourself against possible identity theft is available at https://www.usa.gov/identity-theft.

Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at https://oag.dc.gov/, calling (202) 727-3400, or requesting more information via email oag@dc.gov or mail 400 6th Street NW, Washington DC 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at https://oag.maryland.gov/Pages/oag.aspx, calling the Identity Theft Unit at (410) 576-6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above, and you have rights under the Fair Credit Reporting Act as described above.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the New York State Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: (800) 771-7755.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website at https://ncdoj.gov/protecting-consumers/protecting-your-identity/, calling (919) 716-6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (877) 877-9392 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at (401) 274-4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at https://ago.vermont.gov/.

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

March 10, 2026

Re: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We are writing to notify you of a recent incident that may have impacted your personal information. SitusAMC Holdings Corporation ("SitusAMC") and/or its subsidiaries and affiliates work with various financial institutions to provide certain mortgage-related services that may involve borrower information and, in some cases, non-borrower information in connection with mortgage transactions. This letter explains the circumstances as we understand them and the resources we are making available to you. At this time, we are not aware of any fraudulent use of your personal information as a result of this incident.

What Happened?
On or about November 12, 2025, SitusAMC became aware of unauthorized access to certain systems within its information technology network. Upon becoming aware of the incident, SitusAMC commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and began taking measures to assess and contain the incident.

The investigation has determined that an unauthorized third party acquired data from certain SitusAMC systems between November 13-21, 2025. As part of the review of the impacted data, SitusAMC identified that some of your personal information may have been involved.

What Information May Have Been Involved?
Based on our investigation, the personal information involved may have included your name, address, <<Variable Text 1>>.

What We Are Doing
Upon learning of the incident, we commenced an investigation into the nature and scope of the incident and notified law enforcement. We also took measures to further harden and enhance our security.

What You Can Do
We recommend that you remain vigilant for fraud and identity theft. To help address concerns you may have about this incident, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. To activate these services, please take the following steps:

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code: <<ENROLLMENT>>. Please note the deadline to enroll is June 10, 2026.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at (844) 814-3163 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

We encourage you to review and monitor your accounts for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and immediately report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information
If you have questions about this matter or would like additional information, please call toll-free (844) 814-3163, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time (excluding major bank holidays). You may also email us at SitusAMC@idx.us or write to us at 5065 Westheimer Rd., Suite 700E, Houston, TX 77056, Attention: Legal/Regulatory Office. To help our care team respond promptly, please include your full name, a phone number where you can be reached, and a brief description of your question or the assistance you are requesting.

Sincerely,

SitusAMC

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some steps you may consider:

Reviewing Your Accounts and Credit Reports
Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements and periodically obtain your credit report from each of the three national credit reporting companies. Those companies are:

Equifax P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 Equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 Experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 Transunion.com

Under federal law, you are entitled to obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert
A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report
A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will require you to create or provide you with a credential (such as a PIN number or a password) when you place a security freeze. You will need that credential to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft
If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and report suspected incidents of identity theft online at www.IdentityTheft.gov. You can also file a report by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, fraudulent, or unverifiable information. You can find more information about your rights under the FCRA online at https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Additional guidance on how to help protect yourself against possible identity theft is available at https://www.usa.gov/identity-theft.

P.O. Box 989728
West Sacramento, CA 95798-9728

Parent or Legal Guardian of:
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

March 10, 2026

Re: NOTICE OF DATA BREACH

To the Parent or Legal Guardian of <<First Name>> <<Last Name>>:

We are writing to notify you of a recent incident that may have impacted your child's personal information. SitusAMC Holdings Corporation ("SitusAMC") and/or its subsidiaries and affiliates work with various financial institutions to provide certain mortgage-related services that may involve borrower information and, in some cases, non-borrower information in connection with mortgage transactions. <<Variable Text 1>> This letter explains the circumstances as we understand them and the resources we are making available to your child. At this time, we are not aware of any fraudulent use of your child's personal information as a result of this incident.

What Happened?
On or about November 12, 2025, SitusAMC became aware of unauthorized access to certain systems within its information technology network. Upon becoming aware of the incident, SitusAMC commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and began taking measures to assess and contain the incident.

The investigation has determined that an unauthorized third party acquired data from certain SitusAMC systems between November 13-21, 2025. As part of the review of the impacted data, SitusAMC identified that some of your child's personal information may have been involved.

What Information May Have Been Involved?
Based on our investigation, the personal information involved may have included your child's name, address, <<Variable Text 2>>.

What We Are Doing
Upon learning of the incident, we commenced an investigation into the nature and scope of the incident and notified law enforcement. We also took measures to further harden and enhance our security.

What You Can Do
We recommend that you remain vigilant for fraud and identity theft. To help address concerns you may have about this incident, we are offering identity protection services for your child through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised. To activate these services, please take the following steps:

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your child's Enrollment Code: <<ENROLLMENT>>. Please note the deadline to enroll is June 10, 2026.

Telephone. Contact IDX at (844) 814-3163 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's credit identity.

We encourage you to review and monitor account statements for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and immediately report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect your child against fraud and identity theft.

For More Information

If you have questions about this matter or would like additional information, please call toll-free (844) 814-3163, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time (excluding major bank holidays). You may also email us at SitusAMC@idx.us or write to us at 5065 Westheimer Rd., Suite 700E, Houston, TX 77056, Attention: Legal/Regulatory Office. To help our care team respond promptly, please include your full name and child's name, a phone number where you can be reached, and a brief description of your question or the assistance you are requesting.

Sincerely,

SitusAMC

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some steps you may consider:

Reviewing Your Accounts and Credit Reports
Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements and periodically obtain your credit report from each of the three national credit reporting companies. Those companies are:

Equifax P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 Equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 Experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 Transunion.com

Under federal law, you are entitled to obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert
A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report
A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will require you to create or provide you with a credential (such as a PIN number or a password) when you place a security freeze. You will need that credential to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft
If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and report suspected incidents of identity theft online at www.IdentityTheft.gov. You can also file a report by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, fraudulent, or unverifiable information. You can find more information about your rights under the FCRA online at https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Additional guidance on how to help protect yourself against possible identity theft is available at https://www.usa.gov/identity-theft.

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

February 20, 2026

Re: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We are writing to notify you of a recent incident that may have impacted your personal information. SitusAMC Holdings Corporation ("SitusAMC") and/or its subsidiaries and affiliates work with various financial institutions to provide certain mortgage-related services that may involve borrower information and, in some cases, non-borrower information in connection with mortgage transactions. This letter explains the circumstances as we understand them and the resources we are making available to you. At this time, we are not aware of any fraudulent use of your personal information as a result of this incident.

What Happened?
On or about November 12, 2025, SitusAMC became aware of unauthorized access to certain systems within its information technology network. Upon becoming aware of the incident, SitusAMC commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and began taking measures to assess and contain the incident.

The investigation has determined that an unauthorized third party acquired data from certain SitusAMC systems between November 13-21, 2025. As part of the review of the impacted data, SitusAMC identified that some of your personal information may have been involved.

What Information May Have Been Involved?
Based on our investigation, the personal information involved may have included your name, address, date of birth, <<Variable Text 1>> driver's license number or other government-issued identifier, and/or financial account information (such as bank account number or credit or debit card number). <<Variable Text 2>> Not all data elements were involved for each individual.

What We Are Doing
Upon learning of the incident, we commenced an investigation into the nature and scope of the incident and notified law enforcement. We also took measures to further harden and enhance our security.

What You Can Do
We recommend that you remain vigilant for fraud and identity theft. To help address concerns you may have about this incident, we are offering identity theft protection services through IDX, the data breach and recovery services expert.

IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. To activate these services, please take the following steps:

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code: <<ENROLLMENT>>. Please note the deadline to enroll is May 20, 2026.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at (844) 814-3163 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

We encourage you to review and monitor your accounts for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and immediately report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information
If you have questions about this matter or would like additional information, please call toll-free (844) 814-3163, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time (excluding major bank holidays). You may also email us at SitusAMC@idx.us or write to us at 5065 Westheimer Rd., Suite 700E, Houston, TX 77056, Attention: Legal/Regulatory Office. To help our care team respond promptly, please include your full name, a phone number where you can be reached, and a brief description of your question or the assistance you are requesting.

Sincerely,

SitusAMC

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some steps you may consider:

Reviewing Your Accounts and Credit Reports
Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements and periodically obtain your credit report from each of the three national credit reporting companies. Those companies are:

Equifax P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 Equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 Experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 Transunion.com

Under federal law, you are entitled to obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert
A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report
A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will require you to create or provide you with a credential (such as a PIN number or a password) when you place a security freeze. You will need that credential to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft
If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and report suspected incidents of identity theft online at www.IdentityTheft.gov. You can also file a report by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, fraudulent, or unverifiable information. You can find more information about your rights under the FCRA online at https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Additional guidance on how to help protect yourself against possible identity theft is available at https://www.usa.gov/identity-theft.

Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at https://oag.dc.gov/, calling (202) 727-3400, or requesting more information via email oag@dc.gov or mail 400 6th Street NW, Washington DC 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at https://oag.maryland.gov/Pages/oag.aspx, calling the Identity Theft Unit at (410) 576-6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above, and you have rights under the Fair Credit Reporting Act as described above.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the New York State Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: (800) 771-7755.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website at https://ncdoj.gov/protecting-consumers/protecting-your-identity/, calling (919) 716-6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (877) 877-9392 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at (401) 274-4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at https://ago.vermont.gov/.

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

February 20, 2026

Re: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We are writing to notify you of a recent incident that may have impacted your personal information. SitusAMC Holdings Corporation ("SitusAMC") and/or its subsidiaries and affiliates work with various financial institutions to provide certain mortgage-related services that may involve borrower information and, in some cases, non-borrower information in connection with mortgage transactions. This letter explains the circumstances as we understand them and the resources we are making available to you. At this time, we are not aware of any fraudulent use of your personal information as a result of this incident.

What Happened?
On or about November 12, 2025, SitusAMC became aware of unauthorized access to certain systems within its information technology network. Upon becoming aware of the incident, SitusAMC commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and began taking measures to assess and contain the incident.

The investigation has determined that an unauthorized third party acquired data from certain SitusAMC systems between November 13-21, 2025. As part of the review of the impacted data, SitusAMC identified that some of your personal information may have been involved.

What Information May Have Been Involved?
Based on our investigation, the personal information involved may have included your name, address, <<Variable Text 1>>.

What We Are Doing
Upon learning of the incident, we commenced an investigation into the nature and scope of the incident and notified law enforcement. We also took measures to further harden and enhance our security.

What You Can Do
We recommend that you remain vigilant for fraud and identity theft. To help address concerns you may have about this incident, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. To activate these services, please take the following steps:

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code: <<ENROLLMENT>>. Please note the deadline to enroll is May 20, 2026.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at (844) 814-3163 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

We encourage you to review and monitor your accounts for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and immediately report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information
If you have questions about this matter or would like additional information, please call toll-free (844) 814-3163, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time (excluding major bank holidays). You may also email us at SitusAMC@idx.us or write to us at 5065 Westheimer Rd., Suite 700E, Houston, TX 77056, Attention: Legal/Regulatory Office. To help our care team respond promptly, please include your full name, a phone number where you can be reached, and a brief description of your question or the assistance you are requesting.

Sincerely,

SitusAMC

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some steps you may consider:

Reviewing Your Accounts and Credit Reports
Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements and periodically obtain your credit report from each of the three national credit reporting companies. Those companies are:

Equifax P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 Equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 Experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 Transunion.com

Under federal law, you are entitled to obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert
A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report
A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will require you to create or provide you with a credential (such as a PIN number or a password) when you place a security freeze. You will need that credential to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft
If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and report suspected incidents of identity theft online at www.IdentityTheft.gov. You can also file a report by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, fraudulent, or unverifiable information. You can find more information about your rights under the FCRA online at https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Additional guidance on how to help protect yourself against possible identity theft is available at https://www.usa.gov/identity-theft.