



October 24, 2024

Via E-Mail to: Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

I write on behalf of Stanley Martin Homes, LLC (the “Company”) to provide notice of a security incident potentially affecting 87 Maryland residents.

On September 25, 2024, the Company terminated the employment of one of its human resources employees. That same day, the Company learned that this former employee may have retained Company information following their termination, without the Company’s authorization. The former employee had access to the Company’s human resources databases as part of their job responsibilities while employed. The Company eliminated the employee’s access to the Company’s systems (including the human resources databases) concurrently with the termination. However, upon learning that the former employee may have retained data, the Company took additional steps to confirm that the former employee no longer had access to the Company’s systems, to identify what data the employee accessed during employment, and to investigate the incident with the assistance of a third-party forensic investigation firm and outside consultant. The Company also reported this incident to local and federal law enforcement. The Company’s investigation to date has not confirmed that this former employee actually retained Company information. However, the investigation could not rule out the possibility that the former employee retained some employment-related information in Company files, including the name, Social Security number, date of birth, address, and salary information.

Please note that the Company has not uncovered any information indicating that the personal information of these 87 Maryland residents has been misused in any way. Nevertheless, out of an abundance of caution, we notified all potentially affected Maryland residents on October 24, 2024, and offered them one year of identity theft protection services at no cost to them. A template copy of the notification sent to Maryland residents is attached to this letter.

In addition to contacting law enforcement, the Company is also taking steps to prevent a recurrence, including reviewing relevant security protocols to identify ways to enhance information security.

If you have any questions concerning this matter, please do not hesitate to contact our counsel Ms. Zoe Argento at 303-362-2876 or ZArgento@littler.com.

Sincerely,

A handwritten signature in black ink, appearing to read "J. S. Reed". The signature is stylized with a large, sweeping initial "J" and a long, horizontal stroke extending to the right.

Joel S. Reed
Executive Vice President and General Counsel
Stanley Martin Homes, LLC

STANLEY MARTIN™

HOMES

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[NAME]
[ADDRESS]
[CITY], [STATE], [ZIP CODE]

October 24, 2024

Dear [NAME]:

Stanley Martin Homes, LLC (the "Company") values its current and former employees and takes seriously its obligation to protect your personal information. Unfortunately, we are writing to inform you of a recent information security incident and to share with you the steps that we are taking to address it. While we do not know whether your information has been taken or misused, we are notifying you of this incident as a precaution and because we value transparency.

On September 25, 2024, the Company terminated the employment of a human resources employee. This employee had access to the Company's human resources databases as part of their job responsibilities while employed. We eliminated the employee's access to the Company's systems (including the human resources databases) concurrently with the termination. Shortly after the termination, however, we learned that this former employee may have retained some Company information without authorization. In response, we took additional steps to confirm that the former employee no longer had access to the Company's systems, to identify what data the employee accessed during employment, and to investigate the incident. We also reported this incident to law enforcement.

During our investigation, we were unable to confirm whether this former employee retained or copied Company files, but we were also unable to rule out that possibility. We are notifying you because the files this employee may have retained or copied contained your personal information, including your name, Social Security number, date of birth, address, and salary information. We also want to emphasize that the Company's investigation did not find any indication that your other sensitive information, such as dependent information, health information, or financial or bank account information, was likely impacted. We have no information indicating that your personal information has actually been misused.

Nevertheless, out of an abundance of caution, the Company is offering you one year of identity protection services, at no cost to you, through Experian. This one-year membership in Experian's IdentityWorksSM product provides identity restoration services, fraud detection tools, and other benefits, which include monitoring your credit file at all three nationwide credit bureaus.

You can call Experian's identity restoration agents to assist you to investigate and resolve any incidents of fraud. You may take advantage of this benefit, at any time, until December 31, 2025, by calling Experian at 833-931-7577. No enrollment or activation is necessary. The terms and conditions for identity restoration are located at: www.ExperianIDWorks.com/restoration.

While identity restoration is immediately available to you, you may also activate the fraud detection tools available through IdentityWorks. This product provides you with identity detection, credit monitoring, and resolution of identity theft. If you wish to enroll in IdentityWorks, you will need to do the following:

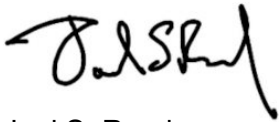
- Ensure that you **enroll by December 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: **[ACTIVATION CODE]**

If you have questions about IdentityWorks, need assistance with identity restoration, or would prefer to enroll in IdentityWorks by telephone, please contact Experian's customer care team at 833-931-7577 by **December 31, 2024**. Be prepared to provide engagement number **[NUMBER]** as proof of eligibility for these services from Experian.

We have also included with this letter additional information on steps you can take to protect the security of your personal information.

The Company regrets this incident and any inconvenience it may cause you. Please be assured that the Company takes seriously both the security of your personal information and this incident. In addition to notifying law enforcement, we are taking the necessary steps to ensure that this does not happen again. If you have any questions or concerns regarding this incident, please call Reena Jacob of our HR team at [PHONE NUMBER].

Sincerely,

A handwritten signature in black ink, appearing to read "Joel S. Reed", written in a cursive style.

Joel S. Reed
Executive Vice President and General Counsel
Stanley Martin Homes, LLC

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in IdentityWorks. You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IdentityWorks membership. Experian's IdentityWorks product will provide the following:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors your credit files at Experian, Equifax, and TransUnion for indicators of fraud.
- **Identity Restoration:** Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE:** You will receive the same high level of identity restoration support even after your IdentityWorks membership expires.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please direct questions about the IdentityWorks product to Experian. A credit card is not required for enrollment in IdentityWorks, and enrollment will not affect your credit score.

2. Review your credit reports. You are entitled to a free copy of your credit report from each of the three national credit bureaus once a week. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You can also receive free credit reports by placing a fraud alert, described below. Errors in information in your credit report, such as a home address or accounts you do not recognize, may be a sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your credit report, whether or not due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

3. Review your account statements. Although we have no reason to believe that your payment or other financial information was impacted by this incident, you should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other services.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from Experian, contact an IdentityWorks identity resolution agent toll-free at 833-931-7577 or visit www.ExperianIDWorks.com/restoration for additional information. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You should also consider reporting such activity to the Company, your local police department, your state's attorney general, and the Federal Trade Commission.

5. You have the right to place a "security freeze" on your credit report. A security freeze will restrict access to your credit file, by prohibiting a consumer reporting agency from releasing information in your credit file without your express consent. This will prevent any unauthorized individuals from opening new credit, loans, or other accounts in your name. However, placing a security freeze on your credit file may also delay or make it more difficult for you to request or apply for a new loan, mortgage, or any other account involving the extension of credit. A security freeze does not apply to existing accounts you have that request information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

There is no charge to place a security freeze. Don't confuse security freezes with "credit locks" or similar programs—they work in similar ways, but credit locks typically come with monthly fees or other expenses. If you want to freeze your credit for free, as guaranteed by federal law, then opt for a security freeze and not a credit lock.

To place a security freeze on your credit file, contact all three of the nationwide credit bureaus, listed below, either online, by mail, or by phone. You will need to provide appropriate proof of your identity including your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. The contact information for all three credit bureaus is:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Woodlyn, PA 19094
1-888-916-8800
www.transunion.com

6. Consider placing a fraud alert with one of the three nationwide credit bureaus. You can place an initial fraud alert by contacting one of the three nationwide credit bureaus listed above. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. To place this alert, a credit bureau will require you to provide appropriate proof of your identity, which may include your Social Security number. If you are the victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide credit bureaus listed above. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address.

7. Additional Information. You may obtain information about fraud alerts and security freezes and additional information about steps you can take to avoid identity theft from the following: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft/; (877) IDTHEFT (438-4338).

If you live in Maryland, please read the additional notice below that applies to you:

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

If you live in North Carolina, please read the additional notice below that applies to you:

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226 (within North Carolina)
1-919-716-6000 (outside of North Carolina)
ncdoj.gov/protecting-consumers/identity-theft/