



Brandon N. Robinson
DIRECT 205.488.3644
EMAIL brandon.robinson@maynardnexsen.com

December 19, 2024

VIA EMAIL ONLY

Attorney General Anthony Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of a Data Security Incident

Dear Attorney General Brown,

Pursuant to Md. Code Ann., Com. Law § 14-3504, I am writing to report a data security incident on behalf of our client, CMH Homes, Inc. ("CMH").

In CMH's retail home centers, it uses multifunction printers that scan home closing documents and send them from the retail center to CMH headquarters in Maryville, TN. In addition, vendor software applications embedded in the printer/scanner digitize the documents, OCR and separate the scans into separate documents, and email them to the CMH headquarters.

On October 25, 2024, CMH discovered that the printer/scanners were additionally copying the transmission to an additional email address appearing to be associated with one of the software vendors, but CMH confirmed that such account was not an account currently maintained by the vendor.

CMH immediately blocked the email account from receiving any future emails, and began an internal audit and review of the documents. CMH also began conducting employee interviews at the affected retail center to determine if a CMH employee had created the email address for a legitimate and authorized purpose. CMH is unaware of the true owner of the blocked account, but its current employees and its vendor deny such ownership. Out of an abundance of caution, CMH is notifying individuals and offering free credit monitoring.

CMH completed its investigation of the records to determine the scope of the breach and identify affected individuals on December 2, 2024. CMH's investigation determined that the personal information of certain CMH customers was impacted, including the personal information of two (2) Maryland residents. The affected information for these individuals included first and last name, driver's license number, and social security number. We are not aware of any actual or attempted misuse of personal information as a result of this incident.

December 19, 2024

Page 2

Following the transmission of this letter, CMH plans to notify affected individuals by written notice by mail, to let them know what happened and to inform them of available resources to monitor and protect their personal information, including 12 months of complimentary credit and identity monitoring services. A template copy of the individual notice is enclosed.

Following the incident, CMH worked with external resources to emphasize compliance with the security policies and procedures in place and to implement security measures designed to prevent a recurrence of such an incident. Specifically, multifunction printers have been secured to prevent the addition of email accounts not associated with CMH or its subsidiaries. As part of its ongoing commitment to information security, CMH will continue to evaluate and prioritize investments in its cybersecurity defenses and continue to conduct due diligence regarding the data security of its individual retail centers.

Please do not hesitate to let me know if you have any questions.

Sincerely,



Brandon N. Robinson



[Return Mail Address]

[Insert Recipient's Name]

[Insert Address]

[Insert City, State, Zip]

[Date]

RE: Important Security Notification. Please read this entire letter.

Dear [First Name] [Last Name]:

We at CMH Homes, Inc. ("CMH") are writing to let you know that one of our retail home centers experienced a data security incident that potentially resulted in unauthorized access to your personal information.

To our knowledge, we are not aware of any actual or attempted misuse of personal information from this incident. However, as a precautionary measure, you have the opportunity to enroll in an identity protection solution through Experian at no cost to you. This service will provide 12 months of credit and identity protection services.

Additional information about the incident, our ongoing response, and the resources that are available to help protect your information can be found below:

What Happened? In CMH's retail home centers, it uses multifunction printer/scanners that scan home closing documents and send them from the retail center to CMH headquarters in Maryville, TN. In addition, vendor software applications embedded in the printer/scanner digitize the documents, OCR and separate the scans into separate documents, and email them to the CMH headquarters.

On October 25, 2024, CMH discovered that the printer/scanners were additionally copying the transmission to an additional email address appearing to be associated with one of the software vendors, but CMH confirmed that such account was not an account currently maintained by the vendor.

CMH immediately blocked the email account from receiving any future emails, and began an internal audit and review of the documents. CMH also began conducting employee interviews at the affected retail center to determine if a CMH employee had created the email address for a legitimate and authorized purpose. CMH is unaware of the true owner of the blocked account, but its current employees and its vendor deny such ownership. Out of an abundance of caution, CMH is notifying individuals, offering free credit monitoring, and it has notified the state attorney general office.

What Are We Doing? CMH values your privacy and deeply regrets that this incident occurred. We have worked with external resources to emphasize compliance with the security policies and procedures in place and to implement security measures designed to prevent a recurrence of such an incident. We are notifying you so that you are aware of what happened here. We believe it is important to be upfront with everyone involved.

What Information Was Involved? Because the documents scanned by the printer/scanner were home closing documents, they contained individual records of certain information input into the CMH's database for business purposes pertaining to customers. Each of these individual records mostly included only simple directory information such as name, address, email address and telephone number. In some limited cases, individual records also appeared to include personal information such as date of birth, social security number (SSN), driver's license number, or other government-issued identification. In addition to your name and contact information, it appears that your record also may have included your [Extra 2] in the documents sent to the unauthorized email address.

What You Can Do? Included in this letter are two resources. First, you will find information enclosed on how to enroll in the 12 months of credit and identity protection services we are offering you through Experian, free of charge, if you are interested in these services. Please follow the instructions enclosed to enroll in such services. Second, we have included an Identity Protection Reference Guide that includes information on general steps you can additionally take to monitor and protect your personal information.

For More Information. If you have any questions or concerns, please email Notifications@ClaytonHomes.com or contact Darrell Jenkins, Chief Information Security Officer, Clayton Homes, at (865) 380-3988.

Sincerely,

CMH Homes, Inc.

DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** April 30, 2025 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **[Activation Code]**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-7577, Monday through Friday from 8:00am to 8:00pm Central Time (excluding major US holidays) by April 30, 2025. Be prepared to provide engagement number B137391 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

** 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.

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-888-4213
Equifax Fraud Alert, P.O. Box 105069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Atlanta, GA 30348-5069	Experian Credit Freeze, P.O. Box 9554,	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094
Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Allen, TX 75013	

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

4. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

5. You can also further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438- 4338); and TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

District of Columbia Residents: You can obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, <https://oag.dc.gov/>.

Iowa Residents: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, <https://www.iowaattorneygeneral.gov/>.

Maryland Residents: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, Identity Theft Unit at: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, 1-888-743-0023 or (410) 576-6491, <https://www.marylandattorneygeneral.gov>.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, <https://www.mass.gov/service-details/identity-theft>.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 114 West Edenton Street, Raleigh, NC, 27603, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, <https://ncdoj.gov/>.

Oregon Residents: You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-877-877-9392 or 503-378-4400, <https://www.doj.state.or.us/>.

Rhode Island Residents: You have the right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, <https://riag.ri.gov/>.