

March 22, 2024

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
VIA EMAIL: IDTheft@oag.state.md.us

Re: Notice Pursuant to MD Commercial Code §14–3501 (e)

Dear Attorney General Brown,

Pursuant to *Maryland Commercial Code section 14–3501 (e)*, we write on behalf of Homeaglow, Inc. (“Homeaglow”), a company that operates an online platform, which connects homeowners with house cleaners, to notify you of a security event involving the credentials for Homeaglow user accounts. We believe this matter potentially involved approximately fifty-two (**52**) Maryland residents. Homeaglow is located at 649 Mission Street, number 313, San Francisco, California 94105.

On or around December 18, 2023, Homeaglow detected an abnormally high volume of login attempts for user accounts on its website and mobile application. Homeaglow swiftly launched an investigation to determine the legitimacy of the activity. This investigation determined that an unauthorized third party appeared to be using credentials in an attempt to access Homeaglow accounts. Homeaglow has identified no evidence that these credentials originated or were obtained from Homeaglow systems or that there was otherwise a compromise of Homeaglow’s systems. Rather, it is Homeaglow’s belief that the third party acquired these credentials from a source outside of Homeaglow and subsequently attempted to identify whether any of the credentials could also be used to access Homeaglow user accounts. In some instances, the credentials were valid, and the third party was able to use them to access the accounts of associated users. After confirming the nature of the event, Homeaglow conducted a comprehensive evaluation to identify the full scope of potentially affected individuals. This process was completed on or around March 5, 2024. Through this review, Homeaglow identified the user accounts of Maryland residents as some of the accounts to which the third party was able to gain access and, in doing so, potentially accessed the personal information stored within the Homeaglow accounts of those residents.

The types of personal information that may have been accessible during this event include information that the Maryland resident provided when creating their Homeaglow account, including the resident’s name, postal address, Social Security number, and any contact information provided to Homeaglow.

Notification of this matter was mailed to the Maryland residents on or around March 22, 2024. There are two versions of this notification letter, both of which are attached. The first version – **Version A** – is intended for individuals who Homeaglow confirmed had their accounts accessed by the unauthorized actor. The second version – **Version B** – is intended for individuals who, during the security event, may have had their account accessed by the unauthorized actor but for whom forensic evidence was not available to confirm such access with any certainty. Homeaglow has not identified any evidence that this second set of individuals were impacted by the security event but is notifying these individuals out of an abundance of caution.



Office of the Attorney General

Page 2

Homeaglow takes the protection of customer information seriously. Upon learning of the event, Homeaglow promptly executed a password reset for all potentially impacted user accounts in an effort to prevent further unauthorized third party access. Homeaglow will also provide two years of identity protection services, at no cost, to affected individuals through IDX.

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

Alex Intile

Alex Intile

AI

VERSION A



4145 SW Watson Avenue
Suite 400, Beaverton, OR 97005

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

March 22, 2024

RE: NOTICE OF SECURITY EVENT

Dear <<First Name>> <<Last Name>>,

We are writing to provide you with information regarding a security event involving the credentials for your account at Homeaglow, Inc. ("Homeaglow"). The event may have resulted in an unauthorized third party accessing or acquiring your personal information contained within your Homeaglow account. We are providing you with information about the event, our response, and steps you may take to help protect against the possibility of identity theft and fraud.

What Happened?

On or around December 18, 2023, Homeaglow detected an abnormally high volume of login attempts for user accounts on our website and mobile application. We swiftly launched an investigation to determine the legitimacy of the activity. Our investigation determined that an unauthorized third party appeared to be using credentials in an attempt to access Homeaglow accounts. We have identified no evidence that these credentials originated or were obtained from Homeaglow systems. Rather, it is our belief that the third party acquired these credentials from a source outside of Homeaglow and subsequently attempted to identify whether any of the credentials could also be used to access a Homeaglow account. In some instances, the credentials were valid, and the third party was able to use them to access the associated Homeaglow user accounts; however, we have not been able to confirm whether the third party actually accessed your personal information within your Homeaglow account during this period. After confirming the nature of the event, we conducted a comprehensive evaluation to identify the full scope of potentially affected individuals. This process was completed on or around March 5, 2024. Through this review, we identified your user account as one of the accounts to which the third party was able to gain access and, in doing so, potentially could have had access to your personal information stored within your Homeaglow account.

What Information Was Involved?

The potentially accessed information includes the information you provided when creating your Homeaglow account. This includes your name, postal address, Social Security number, and any contact information provided to Homeaglow.

What We Are Doing.

We take the protection of your account and your information very seriously. As soon as we learned of the event, we promptly executed a password reset for all potentially impacted user accounts in an effort to prevent further unauthorized third party access. We are also notifying you, so that you may take steps to protect your information. To help you protect your information, we are also offering you two years of identity protection services, at no cost, through IDX.

What You Can Do.

There are steps you can take to help protect your information, including enrolling in an identity protection service we are offering to you for free. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 22, 2024.

For More Information.

In addition to the information provided in this letter, we have also enclosed an attachment with additional information and resources. IDX representatives can answer questions or concerns you may have regarding these services and the protection of your information.

Sincerely,

A handwritten signature in black ink that reads "Xiao Wei Chen". The signature is written in a cursive, flowing style.

Xiao Wei Chen

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax

PO Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian

PO Box 4500
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

PO Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which are actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also

important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For District of Columbia Residents: You may also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia:

Office of the Attorney General for the District of Columbia

Office of Consumer Protection
400 6th Street NW
Washington, D.C. 20001
(202) 442-9828
<https://oag.dc.gov/>

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General

Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
<http://www.marylandattorneygeneral.gov>

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office or New York's Office of Information Technology Services:

New York Attorney General's Office

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
<https://ag.ny.gov/>

New York Office of Information Technology Services

Empire State Plaza
P.O. Box 2062
Albany, NY 12220-0062
844-891-1786
<https://its.ny.gov/>

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General

Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
<https://riag.ri.gov/>

VERSION B



4145 SW Watson Avenue
Suite 400, Beaverton, OR 97005

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

March 22, 2024

RE: NOTICE OF SECURITY EVENT

Dear <<First Name>> <<Last Name>>,

We are writing to provide you with information regarding a security event involving the credentials for your account at Homeaglow, Inc. ("Homeaglow"). The event may have resulted in an unauthorized third party accessing or acquiring your personal information contained within your Homeaglow account. Although at this time there is no indication that your personal information contained within your Homeaglow account has been subject to unauthorized access or misuse in relation to this event, we are providing you with information about the event, our response, and steps you may take to help protect against the possibility of identity theft and fraud.

What Happened?

On or around December 18, 2023, Homeaglow detected an abnormally high volume of login attempts for user accounts on our website and mobile application. We swiftly launched an investigation to determine the legitimacy of the activity. Our investigation determined that an unauthorized third party appeared to be using credentials in an attempt to access Homeaglow accounts. We have identified no evidence that these credentials originated or were obtained from Homeaglow systems. Rather, it is our belief that the third party acquired these credentials from a source outside of Homeaglow and subsequently attempted to identify whether any of the credentials could also be used to access a Homeaglow account. In some instances, the credentials were valid, and the third party was able to use them to access the associated Homeaglow user accounts; however, we have not been able to confirm whether the third party actually accessed your Homeaglow account during this period. After confirming the nature of the event, we conducted a comprehensive evaluation to identify the full scope of potentially affected individuals. This process was completed on or around March 5, 2024.

At this time, we do not have any evidence that the third party was able to access your account or that your personal information was subject to unauthorized access, fraud, or misuse as a result of the event. However, we are notifying you in an abundance of caution because, based on our review, we determined that the third party could potentially have had access to your account during this period and, in doing so, potentially could have had access to your personal information stored within your Homeaglow account.

What Information Was Involved?

The potentially accessed information includes the information you provided when creating your Homeaglow account. This includes your name, postal address, Social Security number and any contact information provided to Homeaglow. At this time, we do not have any evidence that the third party was able to access your account or that your personal information was subject to unauthorized access, fraud, or misuse as a result of the event.

What We Are Doing.

We take the protection of your account and your information very seriously. As soon as we learned of the event, we promptly executed a password reset for all potentially impacted user accounts in an effort to prevent further unauthorized third party access. We are also notifying you so that you may take steps to protect your information. To help you protect your information, we are also offering you two years of identity protection services, at no cost, through IDX.

What You Can Do.

There are steps you can take to help protect your information, including enrolling in an identity protection service we are offering to you for free. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 22, 2024.

For More Information.

In addition to the information provided in this letter, we have also enclosed an attachment with additional information and resources. IDX representatives can answer questions or concerns you may have regarding these services and the protection of your information.

Sincerely,

A handwritten signature in dark ink that reads "Xiao Wei Chen". The signature is written in a cursive, slightly slanted style.

Xiao Wei Chen

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax
PO Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian
PO Box 4500
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
PO Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which are actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if

the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For District of Columbia Residents: You may also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia:

Office of the Attorney General for the District of Columbia

Office of Consumer Protection
400 6th Street NW
Washington, D.C. 20001
(202) 442-9828
<https://oag.dc.gov/>

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General

Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
<http://www.marylandattorneygeneral.gov>

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office or New York's Office of Information Technology Services:

New York Attorney General's Office

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
<https://ag.ny.gov/>

New York Office of Information Technology Services

Empire State Plaza
P.O. Box 2062
Albany, NY 12220-0062
844-891-1786
<https://its.ny.gov/>

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General

Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
<https://riag.ri.gov/>