



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 19, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Ashford, Inc. and its subsidiaries, Inspire, RED Hospitality & Leisure, LLC, Remington Holdings, L.P., Ashford Hospitality Advisors LLC, Ashford Hospitality Services LLC, Ashford Securities LLC, Premier Project Management LLC (collectively, "Ashford"), located at 14185 Dallas Parkway, Suite 1100, Dallas, TX 75254, and are writing to notify your office of an incident suffered by Ashford, Inc. that may affect the security of certain personal information relating to two thousand two hundred ten (2210) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Ashford does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about September 20, 2023, Ashford became aware of suspicious activity on its computer network. Following this, Ashford immediately commenced an investigation with the assistance of computer forensic specialists to secure its systems and determine the nature and scope of the incident. Ashford's investigation determined that an unauthorized actor accessed certain systems in its environment on September 7, 2023, and accessed and acquired certain files stored on these systems during this time. Ashford then undertook a detailed and time-consuming review of the files to determine what data was contained therein and to whom that data relates. On or about November 8, 2023, this review concluded, and Ashford determined that information related to certain individuals was present within the affected files. Since then, Ashford has worked to confirm

the information at issue and locate necessary address information in order to provide an accurate notice.

The information that was impacted by this incident includes name, and Social Security number.

Notice to Maryland Residents

On or about January 19, 2024, Ashford provided written notice of this incident to two thousand two hundred ten (2210) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Ashford moved quickly to investigate and respond to the incident, assess the security of Ashford systems, and identify potentially affected individuals. Further, Ashford notified federal law enforcement regarding the event. Ashford is also working to implement additional safeguards to increase its security posture. Ashford is providing access to credit monitoring services for two (2) years, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Ashford is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Ashford is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Ashford is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/jwn
Enclosure

EXHIBIT A



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

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

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

January 19, 2024

RE: NOTICE OF <<Variable 2>>

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

Ashford, Inc. and its subsidiary, <<Variable 1>> (collectively, "Ashford") are contacting you to notify you of an incident suffered by Ashford, Inc. that affects some of your personal information. We take the security of information in our care seriously, and are providing you with this notice to make you aware of the incident, the steps we are taking in response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On September 20, 2023, Ashford became aware of suspicious activity on our computer network. Following this, we immediately commenced an investigation with the assistance of computer forensic specialists to secure our systems and determine the nature and scope of the incident. Our investigation determined that an unknown and unauthorized actor accessed certain systems in our environment on September 7, 2023, and accessed and acquired certain files stored on these systems during this time. Ashford then undertook a detailed and time-consuming review of the files to determine what data was contained within the files and to whom that data relates. On or about November 8, 2023, this review concluded, and we determined that information related to you was present within the affected files. Since then, we have worked to locate necessary address information in order to provide an accurate notice. We have no evidence of any fraudulent misuse of your information in connection with this incident.

What Information Was Involved? The following types of your information were present in the affected files: your name and <<Variable 3>>. To date, we are unaware of any actual misuse of this information as a result of the event. If information of your dependent(s) was impacted, we are sending you a separate letter for each dependent.

What We Are Doing. Upon discovering this incident, we took immediate steps to further secure our environment and conducted a thorough investigation of the incident. We have also implemented additional safeguards to increase our security posture. We have notified federal law enforcement and other regulators as required. As an added precaution, we are offering you complimentary access to 24 months of credit monitoring services, through IDX, a ZeroFox company. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Protect Personal Information* for additional detail on these services.

What You Can Do. Ashford encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and monitor free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Protect Personal Information* and enroll in the credit monitoring services we are offering. In addition, we encourage you to promptly report any suspected incidents of identity theft to local law enforcement, the Federal Trade Commission, and/or your state Attorney General.

For More Information. If you have questions that are not answered by this letter, please call our dedicated assistance line at (888) 796-3046. This toll-free line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.

We sincerely apologize for this incident and regret any inconvenience it may cause you.

Sincerely,

Ashford, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is April 19, 2024.

2. 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.

3. Telephone. Contact IDX at (888) 796-3046 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

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	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 7 Rhode Island residents that may be impacted by this event.



Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 4, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Ashford, Inc. and its subsidiaries, Inspire, RED Hospitality & Leisure, LLC, Remington Holdings, L.P., Ashford Hospitality Advisors LLC, Ashford Hospitality Services LLC, Ashford Securities LLC, Premier Project Management LLC (collectively, "Ashford") located at 14185 Dallas Parkway, Suite 1100, Dallas, TX 75254, and are writing to supplement our January 19, 2024 notification to your office of an incident that may affect the security of certain personal information relating to an additional one (1) Maryland resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Ashford does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about September 20, 2023, Ashford became aware of suspicious activity on its computer network. Following this, Ashford immediately commenced an investigation with the assistance of computer forensic specialists to secure its systems and determine the nature and scope of the incident. Ashford's investigation determined that an unauthorized actor accessed certain systems in its environment on September 7, 2023, and accessed and acquired certain files stored on these systems during this time. Ashford then undertook a detailed and time-consuming review of the files to determine what data was contained therein and to whom that data relates. On or about November 8, 2023, this review concluded, and Ashford determined that information related to certain individuals was present within the affected files. Since then, Ashford has worked to confirm the information at issue and locate necessary address information in order to provide an accurate notice.

The information that was impacted by this incident includes name and driver's license or state issued identification number.

Notice to Maryland Resident

On January 19, 2024, Ashford provided notice to approximately 2,210 Maryland residents. On or about June 4, 2024, Ashford provided written notice of this incident to an additional 1 Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Ashford moved quickly to investigate and respond to the incident, assess the security of Ashford systems, and identify potentially affected individuals. Further, Ashford notified federal law enforcement regarding the event. Ashford is also working to implement additional safeguards to increase its security posture. Ashford is providing access to credit monitoring services for one (1) year, through IDX, to the individual whose personal information was potentially affected by this incident, at no cost to this individual.

Additionally, Ashford is providing the impacted individual with guidance on how to better protect against identity theft and fraud. Ashford is providing the individual with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Ashford has provided written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/jwn
Enclosure

EXHIBIT A



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

Enrollment Code: KM9MP6YDXC

To Enroll, Visit:

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

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

<<date>>, 2024

NOTICE OF SECURITY INCIDENT

Dear <<Name 1>> <<Name 2>>:

Ashford, Inc. and its subsidiary, <Variable 1> (collectively, "Ashford") are contacting you to notify you of an incident suffered by Ashford, Inc. that affects some of your personal information. We take the security of information in our care seriously, and are providing you with this notice to make you aware of the incident, the steps we are taking in response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On September 20, 2023, Ashford became aware of suspicious activity on our computer network. Following this, we immediately commenced an investigation with the assistance of computer forensic specialists to secure our systems and determine the nature and scope of the incident. Our investigation determined that an unknown and unauthorized actor accessed certain systems in our environment on September 7, 2023, and accessed and acquired certain files stored on these systems during this time. Ashford then undertook a detailed and time-consuming review of the files to determine what data was contained within the files and to whom that data relates. We recently determined that information related to you was present within the affected files. We have no evidence of any fraudulent misuse of your information in connection with this incident.

What Information Was Involved? The following types of your information were present in the affected files: your name and driver's license or state issued identification number. To date, we are unaware of any actual misuse of this information as a result of the event. If information of your dependent(s) was impacted, we are sending you a separate letter for each dependent.

What We Are Doing. Upon discovering this incident, we took immediate steps to further secure our environment and conducted a thorough investigation of the incident. We have also implemented additional safeguards to increase our security posture. We have notified federal law enforcement and other regulators as required. As an added precaution, we are offering you complimentary access to twelve (12) months of credit monitoring services, through IDX, a ZeroFox company. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Protect Personal Information* for additional detail on these services.

What You Can Do. Ashford encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and monitor free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Protect Personal Information* and enroll in the credit monitoring services we are offering. In addition, we encourage you to promptly report any suspected incidents of identity theft to local law enforcement, the Federal Trade Commission, and/or your state Attorney General.

For More Information. If you have questions that are not answered by this letter, please call our dedicated assistance line at 1-800-939-4170. This toll-free line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.

We sincerely apologize for this incident and regret any inconvenience it may cause you.

Sincerely,
Ashford, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is March 1, 2025.
2. 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.
3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

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	1-800-916-8800

Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Ashford, Inc. is located at 14185 Dallas Parkway, Suite 1200, Dallas, TX 75254.