EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, East West Family of Companies ("EW") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 8, 2021, EW discovered unauthorized access to certain computer systems on its network. EW immediately took steps to secure its systems and launched an investigation with the assistance of third-party computer forensic specialists to determine what may have happened. EW also worked extensively to restore system operations. The investigation determined that an unknown actor gained access to certain computer systems on the network, and between November 5 and November 8, 2021, accessed and/or acquired certain files from these systems. Although EW has no evidence of any identity theft or fraud in connection with this incident, EW reviewed the files at issue and on or about May 9, 2022, determined that some of the affected files contained information of current and former employees and their dependents. EW has worked since this time to gather current address information and prepare an accurate notification to those who may be affected by this incident.

The information that may be affected by this incident includes name and Social Security number.

Notice to Maine Residents

On July 1, 2022, EW provided written notice of this incident to five (5) Maine 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, EW moved quickly to investigate and respond to the incident, assess the security of EW systems, and identify potentially affected individuals. Further, EW notified federal law enforcement regarding the event. EW is providing access to credit monitoring services for one (1) year, through Experian to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, EW is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. EW 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. EW 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.

EXHIBIT A

EAST WEST

FAMILY OF COMPANIES

east west partners | SLIFER SMITH & FRAMPTON | Forbes | eastwest HOSPITALITY

Return Mail Processing
PO Box 999
Suwanee, GA 30024

39 1 8927 **********AUTO**ALL FOR AADC 894
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

July 1, 2022

NOTICE OF [Extra3]

Dear Sample A. Sample:

East West Family of Companies ("EW") is writing to notify you of an incident that may have impacted the privacy of some of your information. Although we have no evidence of any identity theft or fraud occurring as a result of this incident, this letter provides an overview of the incident, our response, and resources available to you to help protect your information, should you feel it is appropriate to do so.

What Happened? On November 8, 2021, EW discovered unauthorized access to certain computer systems on our network. We immediately took steps to secure our systems and launched an investigation with the assistance of third-party computer forensic specialists to determine what may have happened. We also worked extensively to restore system operations. The investigation determined that an unknown actor gained access to certain computer systems on our network, and between November 5 and November 8, 2021, accessed and/or acquired certain files from these systems. Although we have no evidence of any identity theft or fraud in connection with this incident, we reviewed the files at issue and on or about May 9, 2022, determined that some of the affected files contained information of our current and former employees and their dependents, including you. We have worked since this time to gather current address information and prepare an accurate notification to those who may be affected by this incident.

What Information Was Involved? Our investigation determined your name and Social Security number may have been impacted by this incident. We have no evidence that your specific information was actually viewed, and we have no evidence of any actual or attempted fraudulent use of your information resulting from this incident. If information of your dependent(s) was involved, we are providing separate notifications to you for each dependent.

What We Are Doing. We take this incident and the security of information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, and to secure our environment. Our response included resetting relevant account passwords, reviewing the contents of the potentially accessed files and folders to determine whether they contained personal information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information, we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. Law enforcement has also been notified of this event.

We are also offering you access to complimentary credit monitoring and identity protection services for [Extra4] months through Experian. These services include fraud consultation and identity theft restoration services. If you wish to activate the credit monitoring and identity protection services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*. There you will also find more information on the complimentary credit monitoring services we are making available to you. While EW will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (833) 420-2822 toll-free Monday through Friday from 8 am - 10 pm Central, or Saturday and Sunday from 10 am - 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number [Engagement Number]. You may also write to EW at P.O. Box 9550, Avon, CO 81620.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Colleen Weiss,
Chief Executive Officer
East West Hospitality

Jason Cole
Chief Executive Officer
Slifer Smith and Frampton

Chris Frampton
Chief Executive Officer
East West Partners

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring and Identity Restoration Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for [Extra4] 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 [Extra4] 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 [Extra4] 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 September 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your **activation code**: **ABCDEFGHI**

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) 420-2822** by **September 30, 2022**. Be prepared to provide engagement number **[Engagement Number]** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra4] 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 ExtendCARE™:** 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.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

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.);
7. Social Security card, W2, or paystub;
8. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, 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	1-833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud and obtain a copy of the report. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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, DC 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; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.