EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Jewish Community Federation ("The Federation") does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data event notification statute, or personal jurisdiction.

Nature of the Data Event

The Federation first learned of potentially suspicious activity related to certain employee email accounts in October 2018. The Federation then launched an investigation to determine the full nature and scope of the suspicious activity. Through a detailed and exhaustive investigation, on February 19, 2019, the Federation learned that an unknown actor(s) gained access to certain Federation employee email accounts as the result of a phishing attack. The employees' email credentials were changed, and the email accounts have been secured. A leading forensic investigation firm was retained to assist with the investigation into what happened and what information contained within the email accounts may have been affected. The investigation determined that an unknown individual had accessed certain Federation employees' email accounts as early as September 12, 2018.

Since the investigation was unable to determine if any emails were viewed, The Federation reviewed the entire contents of the relevant email accounts through a manual and programmatic process to determine whether personal information may have been present in the email accounts at the time of the incident. On April 17, 2019, it was confirmed that personal information was contained in the accounts. The Federation conducted a review, confirming the identities of the individuals impacted, as well as the impacted data elements and relevant address information, which was completed on September 17, 2019.

The information that could have been subject to unauthorized access includes name, address, Social Security number, financial account information, credit card information, Driver's License number, and medical information.

Notice to California Residents

On or about September 24, 2019, The Federation provided written notice of this incident to all affected individuals, which includes one thousand sixty-seven (1067) California 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, The Federation investigate and respond to the incident, assessed the security of The Federation systems, and notified potentially affected individuals. The Federation is also working to implement additional safeguards and training to its employees. The Federation is providing access to credit monitoring services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, The Federation 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. The Federation 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.

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

The Jewish Community Federation ("The Federation") discovered that it became the target of a phishing email campaign that compromised several Federation email account credentials. We are writing to provide you with information on the incident, steps we are taking in response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate.

What Happened? We learned of suspicious activity related to certain employee email accounts. We then launched an investigation to determine the full nature and scope of this incident. Through a detailed and exhaustive investigation, we confirmed that an unknown actor(s) gained access to certain Federation employee email accounts as the result of a phishing attack. The employees' email credentials were changed, and the email accounts have been secured. A leading forensic investigation firm was immediately retained to assist with our investigation into what happened and what information contained within the email accounts may have been affected. The investigation determined that an unknown individual had accessed certain Federation employees' email accounts as early as September 12, 2018.

Since the investigation is unable to determine if any emails were viewed, we reviewed the contents of the relevant email accounts through a manual and programmatic process to determine whether personal information may have been present in the email accounts at the time of the incident. On April 17, 2019, it was confirmed that personal information was contained in the accounts. We conducted a review, confirming the identities of the individuals, impacted data elements and relevant address information, which was completed on July 30, 2019.

What Information Was Involved? Our investigation determined that your personal information was present in an affected email account at the time of the incident. This personal information includes your <<ClientDef1(Breach Details)>>. Please note that while our investigation did not reveal evidence that your information was actually viewed by the unauthorized actor, we are providing you this notice to ensure you are aware of this incident.

What We Are Doing. Information privacy and security are among our highest priorities. The Federation has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems. We reset passwords for all relevant Federation accounts and systems, are reviewing our policies and procedures relating to data security and are conducting additional employee training.

In an abundance of caution, we are notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. We have arranged to have Kroll provide identity monitoring services for 12 months at no cost to you as an added precaution. We are also reporting the event to relevant state regulators.

What You Can Do. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." You may also activate to receive the identity monitoring services we are making available to you. The Federation will cover the cost of this service. Because the activation process does not allow us to activate on your behalf, you will need to activate yourself by following the instructions outlined in this letter.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-389-2397 (toll free), Monday through Friday, 9:00 a.m. to 6:30 p.m., ET. You may also write to us at Jewish Community Federation and Endowment Fund, 121 Steuart Street, San Francisco, CA, 94105.

We sincerely regret any inconvenience this incident may cause you. The Federation remains committed to safeguarding information in our care and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

Holden Lee
Chief Financial and Investment Officer
Jewish Community Federation

Steps You Can Take to Protect Your Information

Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **December 11, 2019** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect error over the next 12 to 24 months. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	PO Box 105788 Atlanta, GA 30348-5788 1-800-349-9960 www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

You can 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, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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. 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. This notice has not been delayed by law enforcement.

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

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 agencies 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 Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 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.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.