

c/o Return Processing Center
P.O. Box 3826
Suwanee, GA 30024



VIA FIRST-CLASS MAIL

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

***Postal IMB Barcode

<<Date>>

Notice of Data <<Variable Data 1>>

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

Hebrew Home for Aged Disabled d/b/a San Francisco Campus for Jewish Living ("SFCJL") is writing to inform you of a recent data incident that may have resulted in unauthorized access to your personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On December 27, 2024, SFCJL discovered that an unauthorized user gained access to an employee's e-mail user account (the "Incident"). Upon discovery of the Incident, SFCJL promptly secured the e-mail account and engaged a specialized cybersecurity incident response firm to investigate and determine the cause and scope of the unauthorized activity. The forensic investigation, which concluded on February 6, 2025, determined that an unauthorized user gained limited access to one (1) employee e-mail user account.

Based on these findings, SFCJL conducted a review of the information that was potentially accessed by the unauthorized user to identify the specific individuals and the types of information that may have been affected by the Incident. On April 1, 2025, SFCJL finalized the list of individuals to notify.

What Information Was Involved?

Based on the investigation, the following information related to you may have been subject to unauthorized access: name; address; <<Breached Elements>>.

Please note the Incident did not involve your Social Security number or your financial information. Further, SFCJL has received no evidence to date that any personal information has been misused by third parties as a result of this incident.

What We Are Doing

Data privacy and security is among SFCL's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since discovery of the incident, SFCJL moved quickly to investigate, respond, and confirm the security of its systems. Specifically, SFCJL changed all user credentials, enhanced its data security measures, notified law enforcement, and took steps and will continue to take steps to mitigate the risk of future harm.

In light of the incident, we are also providing you with <<CM Duration>> months of complimentary credit monitoring and identity theft restoration services through HaystackID. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do

You may activate the credit monitoring services we are making available to you at no cost. The deadline to enroll is <<Enrollment Deadline>>. To enroll in Credit Monitoring services at no charge, please log on to www.privacysolutions.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Activation Code>>

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION*, to learn more about how to protect against the possibility of information misuse.

We would like to reiterate, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 855-549-2666 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

SFCJL sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

San Francisco Campus for Jewish Living

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The agency you contact will then contact the other credit agencies.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting <http://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.

New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at <https://dos.nysits.acsitefactory.com/consumerprotection>; by visiting the New York Attorney General at <https://ag.ny.gov> or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or <https://www.identitytheft.gov/#/>.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting <https://oag.dc.gov>, or emailing at consumer.protection@dc.gov.

c/o Return Processing Center
P.O. Box 3826
Suwanee, GA 30024



VIA FIRST-CLASS MAIL

Postal Endorsement Line
REPRESENTATIVE OF THE ESTATE OF
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
***Postal IMB Barcode

<<Date>>

Notice of Data <<Variable Data 1>>

Dear Representative of the Estate of <<First Name>> <<Last Name>>,

Hebrew Home for Aged Disabled d/b/a San Francisco Campus for Jewish Living (“SFCJL”) is writing to inform you of a recent data incident that may have resulted in unauthorized access to the deceased’s personal information. We sincerely apologize for any impact this Incident may have in connection with your loss. While we are unaware of any fraudulent misuse of the deceased’s personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of the deceased’s information.

What Happened?

On December 27, 2024, SFCJL discovered that an unauthorized user gained access to an employee’s e-mail user account (the “Incident”). Upon discovery of the Incident, SFCJL promptly secured the e-mail account and engaged a specialized cybersecurity incident response firm to investigate and determine the cause and scope of the unauthorized activity. The forensic investigation, which concluded on February 6, 2025, determined that an unauthorized user gained limited access to one (1) employee e-mail user account.

Based on these findings, SFCJL conducted a review of the information that was potentially accessed by the unauthorized user to identify the specific individuals and the types of information that may have been affected by the Incident. On April 1, 2025, SFCJL finalized the list of individuals to notify.

What Information Was Involved?

Based on the investigation, the following information related to the deceased may have been subject to unauthorized access: name; address; <<Data Elements>>.

Please note the Incident did not involve the deceased’s Social Security number or financial information. Further, SFJCL has received no evidence to date that any personal information has been misused by third parties as a result of this incident.

What We Are Doing

Data privacy and security is among SFCL's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since discovery of the incident, SFCJL moved quickly to investigate, respond, and confirm the security of its systems. Specifically, SFCJL changed all user credentials, enhanced its data security measures, notified law enforcement, and took steps and will continue to take steps to mitigate the risk of future harm.

In light of the incident, we are also providing you with <<CM Duration>> months of complimentary credit monitoring and identity theft restoration services through HaystackID. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do

You may activate the credit monitoring services we are making available to you at no cost. The deadline to enroll is <<Enrollment Deadline>>.

To enroll in Credit Monitoring services at no charge, please log on to www.privacysolutions.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Activation Code>>

In order for the decedent to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for the decedent's own protection to confirm the decedent's identity.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review the deceased's account statements and to monitor the deceased's credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact the deceased's financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect the estate's interests, including the possible closure of the deceased's credit file. Please review the enclosed *ADDITIONAL RESOURCES TO HELP PROTECT THE DECEDENT'S INFORMATION*, to learn more about how to protect against the possibility of information misuse.

We would like to reiterate, at this time, there is no evidence that the deceased's information was misused as a result of the Incident. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 855-549-2666 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

SFCJL sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

San Francisco Campus for Jewish Living

ADDITIONAL RESOURCES TO HELP PROTECT THE DECEDENT'S INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing the decedent's credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with the decedent's information or if you do not recognize any of the account activity.

You may obtain a free copy of the decedent's credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of the decedent's credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about the decedent's rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on the decedent's credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing the decedent's credit file without the decedent's consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on the decedent's credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on the decedent's credit file at no cost. A fraud alert is a statement that is added to the decedent's credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify the decedent's identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify the decedent's identity before extending new credit, but it does not block access to the decedent's credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending the decedent's request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect the decedent against identity theft, you can contact the Federal Trade Commission (FTC) 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting <http://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at <https://dos.nysits.acsitefactory.com/consumerprotection>; by visiting the New York Attorney General at <https://ag.ny.gov> or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or <https://www.identitytheft.gov/#/>.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting <https://oag.dc.gov>, or emailing at consumer.protection@dc.gov.