

Children's Council of San Francisco
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2722



Name

Address

City, State Zip Code



February 27, 2026

Re: Notice of Data Security Incident

Dear Name:

We are writing to inform you of a recent data security incident that involved your personal information. Children's Council of San Francisco ("ChCo") takes the privacy and security of all information within its possession very seriously. Please read this letter carefully, as it contains important information regarding the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? We recently determined that some of your personal information was involved in a data security incident. On August 3, 2025, ChCo experienced a network disruption. We immediately took steps to secure our network and engaged cybersecurity experts to conduct an investigation. The investigation determined that an unknown actor accessed and acquired certain data without authorization. We then engaged a third-party vendor to conduct a comprehensive review of the affected data to determine whether personal information may have been involved. Following a thorough review of the data impacted, on NCOA Date, ChCo confirmed the scope of the data impacted and secured information sufficient to effectuate notice. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved? The data involved included your name in combination with your Social Security Number.

What We Are Doing: As soon as we discovered this incident, we took the steps described above and implemented measures to enhance our network security to minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will cooperate with any resulting investigation.

Additionally, we are offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services, including a \$1,000,000 identity theft insurance policy, at no charge to you. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services are provided through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in the credit monitoring and identity theft protection services at no charge to you, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: Code

In order for you to receive the 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.

What You Can Do: You can follow the recommendations on the following page to help protect your information. You can also enroll in the complementary services offered to you through TransUnion by using the enrollment code provided above.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call TransUnion at 1-866-916-5125 from 5:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday (excluding holidays). TransUnion representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Sincerely,

Children's Council of San Francisco
445 Church Street
San Francisco, CA 94114

Additional Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9701, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit:

http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

California: California Attorney General can be reached at: 1300 I Street, Sacramento, CA 95814; 800-952-5225; www.oag.ca.gov/privacy

Iowa: Iowa Attorney General can be reached at: 1305 E. Walnut St., Des Moines, IA 50319; 888-777-4590; www.iowaattorneygeneral.gov

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

Oregon: Oregon Attorney General can be reached at: 1162 Court St., NE, Salem, OR 97301; 877-877-9392; www.doj.state.or.us/consumer-protection

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

Washington D.C.: Washington D.C. Attorney General can be reached at: 400 S 6th Street, NW Washington, DC 20001 www.oag.dc.gov 1-202-727-3400



Children's Council de San Francisco
Atención Cyberscout
555 Monster Rd SW
Renton, WA 98057



Name
Address
City, State Zip Code

27 de febrero de 2026

Ref.: Aviso de incidente de datos incidente de seguridad

Estimado/a Name:

Nos comunicamos con usted para informarle acerca de un reciente incidente de seguridad de datos que involucró su información personal. Children's Council of San Francisco ("ChCo") toma muy seriamente la privacidad y la seguridad de toda la información que tiene en su poder. Lea esta carta detenidamente, ya que contiene información importante sobre el incidente y los recursos que puede utilizar para proteger su información, que incluye las instrucciones para inscribirse en los servicios gratuitos de monitoreo de crédito y protección contra robo de identidad.

¿Qué sucedió? Recientemente, hemos determinado que parte de su información personal estuvo involucrada en un incidente de seguridad de datos. El 3 de agosto de 2025, ChCo experimentó una interrupción en la red. Inmediatamente tomamos medidas para proteger nuestra red y contratamos a expertos en ciberseguridad para llevar a cabo una investigación. La investigación determinó que un actor desconocido accedió y adquirió ciertos datos sin autorización. A continuación, contratamos a un proveedor externo para que realice una revisión exhaustiva de los datos afectados para determinar si la información personal podría haber estado implicada. Después de dicha revisión exhaustiva de datos afectados, en la Fecha de NCOA, ChCo confirmó el alcance de los datos afectados y obtuvo información suficiente para efectuar la notificación. Luego tomamos medidas para notificarle del incidente lo antes posible.

¿Qué información se vio involucrada? Los datos involucrados podrían haber incluido su nombre en combinación con el número de Seguro Social, número de licencia de conducir o de identificación estatal, número de identificación fiscal, número de registro de extranjero/USCIS, número de pasaporte, información médica personal, número de identificación del seguro médico o número de grupo de seguro médico.

Lo que estamos haciendo: Apenas descubrimos este incidente, tomamos las acciones descritas anteriormente e implementamos medidas para mejorar la seguridad de nuestra red a fin de minimizar el riesgo de que se produzca un incidente similar en el futuro. También notificamos a la Oficina Federal de Investigación y cooperaremos con cualquier investigación resultante.

Además, le ofrecemos la oportunidad de inscribirse en servicios de monitoreo de crédito y protección contra robo de identidad sin cargo, incluida una póliza de seguro contra robo de identidad de \$1,000,000, sin cargo para usted. Estos servicios le proporcionan alertas durante 12 meses a partir de la fecha de inscripción cuando se producen cambios en su historial de crédito. Esta notificación se le envía a usted el mismo día en que se produce el cambio o la actualización en la agencia. Por último, le proporcionamos asistencia proactiva contra el fraude para brindarle ayuda ante cualquier pregunta que pueda tener o en caso de que sea víctima de fraude. Estos servicios serán proporcionados a través de Cyberscout, una empresa de TransUnion especializada en asistencia contra el fraude y en servicios de reparación.

Para inscribirse en los servicios de monitoreo de crédito y de protección contra robo de identidad sin cargo, inicie sesión en <https://bfs.cyberscout.com/activate> y siga las instrucciones proporcionadas. Cuando se le solicite, proporcione el siguiente código individual para recibir servicios: Code.

Para que usted pueda recibir los servicios descritos anteriormente, debe inscribirse en el transcurso de 90 días a partir de la fecha de esta carta. La inscripción requiere una conexión a Internet y una cuenta de correo electrónico,

y podría no estar disponible para menores de 18 años. Tenga en cuenta que al registrarse en los servicios de monitoreo, es posible que se le pida que verifique información personal para su propia protección con el fin de confirmar su identidad.

Qué puede hacer usted: Puede seguir las recomendaciones de la página siguiente para ayudar a proteger su información. También puede inscribirse en los servicios de cortesía que se le ofrecen a través de TransUnion utilizando el código de inscripción proporcionado anteriormente.

Cómo obtener más información: En la siguiente página, encontrará más información sobre cómo proteger su información personal. Si tiene preguntas o necesita ayuda, llame a TransUnion al 1-866-916-5125 de 5:00 a. m. a 5:00 p. m., hora del Pacífico, de lunes a viernes (excepto los feriados). Los representantes de TransUnion han tenido total conocimiento del incidente y pueden ayudarle a responder a preguntas que pueda tener con respecto a la protección de su información.

Atentamente,

Children's Council of San Francisco
445 Church Street
San Francisco, CA 94114

Medidas adicionales que puede tomar para proteger mejor su información

Revise sus estados de cuenta y notifique a las autoridades del orden público sobre cualquier actividad sospechosa: Como medida de precaución, le recomendamos que preste atención: revise sus estados de cuenta y monitoree atentamente los historiales de crédito gratis para detectar errores, y tome otras medidas adecuadas para proteger las cuentas, lo que incluye cambiar sus contraseñas oportunamente. Si detecta alguna actividad sospechosa en una cuenta, debe notificar de inmediato a la institución financiera o compañía con la que mantiene la cuenta para obtener asistencia con la reparación o para comunicarse con un proveedor de servicios de reparación. También debe informar de inmediato cualquier actividad fraudulenta o cualquier sospecha de incidencia de robo de identidad a las autoridades del orden público correspondientes, al fiscal general de su estado o a la Comisión Federal de Comercio (Federal Trade Commission, FTC). Además, debe ponerse en contacto con las autoridades del orden público locales y presentar una denuncia policial. Obtenga una copia de la denuncia policial porque es posible que se le pida que proporcione copias a los acreedores para corregir sus registros. La información de contacto de la FTC es la siguiente:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copia del historial de crédito: Puede obtener una copia gratuita de su historial de crédito cada 12 meses de cada una de las tres principales agencias de historial de crédito visitando <http://www.annualcreditreport.com/>, llamando al 1-877-322-8228, o completando un Formulario de solicitud de historial de crédito anual y enviándolo por correo postal a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348. Puede imprimir este formulario en <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. También puede comunicarse con una de las siguientes tres agencias nacionales de historial de crédito:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9701, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Alerta de fraude: Existen dos tipos de alertas de fraude generales que puede colocar en su historial de crédito: una alerta inicial y una alerta extendida. Es posible que desee considerar la posibilidad de colocar una o ambas alertas de fraude en su historial de crédito. Una alerta de fraude inicial es gratuita y permanecerá en su historial de crédito durante al menos 90 días. La alerta informa a los acreedores sobre una posible actividad fraudulenta dentro de su historial y solicita que el acreedor se comunique con usted antes de establecer cualquier cuenta a su nombre. Es posible que se le coloque una alerta extendida en su informe de crédito si ya ha sido víctima de robo de identidad y que proporcione la prueba documental adecuada. Una alerta de fraude extendida también es gratuita y permanece en su historial de crédito durante siete años. Para colocar una alerta de fraude en su informe de crédito, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas más arriba. Puede encontrar más información en <http://www.annualcreditreport.com>. Los miembros de las fuerzas armadas también pueden colocar una Alerta de fraude para militares en servicio activo en sus informes de crédito mientras estén en servicio. Una alerta de fraude para militares en servicio activo dura un año y puede renovarse mientras dure su despliegue.

Congelamientos de crédito o de seguridad: En virtud de la ley de los EE. UU., usted tiene derecho a colocar en su informe crediticio un congelamiento de crédito, también conocido como congelamiento de seguridad, durante un máximo de un año sin costo. El congelamiento evitará que se abra un nuevo crédito a su nombre sin el uso de un número PIN que se le emita cuando inicie el congelamiento. Un congelamiento de seguridad está diseñado para evitar que los potenciales acreedores accedan a su historial de crédito sin su consentimiento. Como consecuencia, el uso de un congelamiento de seguridad puede interferir o retrasar su capacidad para obtener crédito.

Debe colocar por separado el congelamiento de seguridad en su informe crediticio con cada agencia de historial de crédito. No se cobra ningún cargo por colocar o levantar un congelamiento de seguridad. Para obtener información e instrucciones sobre cómo colocar un congelamiento de seguridad, comuníquese con cualquiera de las agencias de historial de crédito o con la FTC identificada anteriormente. A fin de colocar un congelamiento de seguridad, es posible que se le solicite que proporcione a la agencia de historial de crédito del consumidor información que le identifique, incluidos su nombre completo, número de Seguro Social, fecha de nacimiento, direcciones actuales y anteriores, una copia de su tarjeta de identificación emitida por el estado y una factura de servicios públicos,

estado de cuenta bancaria o estado de cuenta del seguro recientes. Después de recibir su solicitud de congelamiento, cada agencia de información crediticia le proporcionará un PIN o contraseña únicos. Guarde el PIN o la contraseña en un lugar seguro, ya que lo necesitará si decide levantar el congelamiento.

El congelamiento se mantendrá hasta que usted solicite a la agencia de información crediticia que lo levante temporalmente o lo elimine por completo. Si la solicitud se realiza por Internet o por teléfono, la agencia de historial crediticio debe levantar el congelamiento de crédito en el plazo de una hora. Si la solicitud se realiza por correo, la agencia debe levantar el congelamiento a más tardar en tres días hábiles después de recibir su solicitud.

PIN de protección de identidad del IRS: Puede obtener un PIN de protección de identidad (IP PIN) del IRS que impida que otra persona presente una declaración de impuestos utilizando su número de Seguro Social. Solo usted y el IRS conocerán su IP PIN, y esto ayudará al IRS a verificar su identidad cuando presente su declaración de impuestos electrónica o impresa. Puede obtener más información y su IP PIN aquí: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

Usted también tiene ciertos derechos en virtud de la Ley de Informe Justo de Crédito (FCRA): Estos derechos incluyen el derecho a saber qué información se incluye en su archivo; a disputar información incompleta o inexacta; a obligar a las agencias de historial de crédito del consumidor a corregir o eliminar información inexacta, incompleta o no verificable. Para obtener más información sobre la FCRA y sus derechos en virtud de la FCRA, visite: http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Recursos adicionales gratuitos: Puede obtener información de las agencias de historial de crédito del consumidor, la FTC o de su respectivo fiscal general del estado sobre alertas de fraude, congelamientos de seguridad y medidas que puede tomar para prevenir el robo de identidad. Puede denunciar presuntos incidentes de robo de identidad a las autoridades del orden público locales, así como a FTC o al fiscal general de su estado.

Más información:

California: Puede comunicarse con el fiscal general de California en: 1300 I Street, Sacramento, CA 95814; 800-952-5225; www.oag.ca.gov/privacy

Iowa: Puede comunicarse con el fiscal general de Iowa en: 1305 E. Walnut St., Des Moines, IA 50319; 888-777-4590; www.iowaattorneygeneral.gov

Maryland: Puede comunicarse con el fiscal general de Maryland en: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us o IDTheft@oag.state.md.us

Oregón: Puede comunicarse con el fiscal general de Oregón en: 1162 Court St., NE, Salem, OR 97301; 877-877-9392; www.doj.state.or.us/consumer-protection

Nueva York: Puede comunicarse con el fiscal general de Nueva York en: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Carolina del Norte: Puede comunicarse con la Oficina del Fiscal General de Carolina del Norte - División de Protección al Consumidor en: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (línea gratuita dentro de Carolina del Norte); 919-716-6000; www.ncdoj.gov

Washington D.C.: Puede comunicarse con el fiscal general de Washington D.C. en: 400 S 6th Street, NW Washington, DC 20001 www.oag.dc.gov 1-202-727-3400



Children's Council of San Francisco (三藩市兒童委員會)

抄報 Cyberscout

555 Monster Rd SW

Renton, WA 98057



Name

Address

City, State Zip Code

2026 年 2 月 27 日

事由：數據通知 保安事件

尊敬的 **Name**：

我們特此致函，通知您一宗最近發生的涉及您個人資料的數據安全事件。三藩市兒童委員會（「ChCo」）非常重視其所保管一切資料的私隱及安全。請細讀本函，因為當中含有關於該事件的重要資料以及您可用以保護您個人資料的多種資源，包括有關登記加入免費信用監控及身份防盜服務的指示。

發生了甚麼事？我們最近確定，您的部分個人資料受到了一宗數據安全事件的波及。ChCo 在 2025 年 8 月 3 日經歷了網絡中斷。我們迅即採取了保護我們網絡的步驟，並聘請網絡安全保障專家展開調查。調查確定，有身份不明分子未經授權而存取並取得了某些數據。我們隨後聘請第三方供應商對受到影響的數據進行全面審查，以確定當中是否有否累及個人資料。在對受影響的數據進行徹底審查後，ChCo 在 NCOA 日期確認了受到影響的數據範圍，並取得充足資料以相應發出通知。我們接著採取措施，盡快將此事件通知您。

涉及哪些資料？所涉及的數據可能包括您的姓名連同社會保障號碼、駕照號碼或州 ID 號碼、稅號、USCIS/外國人登記號碼、護照號碼、個人健康資料、健康保險 ID 號碼，或健康保險團體號碼。

我們如何應對：一經發現此事件，我們便執行了上述應對步驟，還採取了增強網絡安全的措施，以最大限度降低未來發生類似事件的風險。我們亦通知了聯邦調查局，並將配合因之產生的任何調查。

而且，我們正為您提供登記加入免費信用監控及身份防盜保護服務的機會，其中包括價值 \$1,000,000 的身份防盜保單，無需您支付費用。當您的信用檔案出現變動時，這些服務會從登記之日起 <<service length>> 個月內為您提供警訊。此通知將在公司發生變動或更新的同一天發送給您。最後，我們會為您提供適切的反詐騙支援，以幫助解答您可能存有的任何疑問，或協助受騙的您。這些服務通過 TransUnion 旗下公司 Cyberscout 提供，該公司專門從事反欺詐援助和補救服務。

如要免費登記加入信用監控和身份防盜服務，請登錄<https://bfs.cyberscout.com/activate>，並按照指示操作。請根據指示，提供以下唯一識別碼以獲取服務：**Code**。

為了讓您得用上述服務，您必須在本函簽發日期起 90 日內報名登記。登記需要網絡連線和電郵帳戶，且不適用於 18 歲以下的未成年人。請注意，登記監控服務時，您可能被要求驗證個人資料，以自我保護並確認您的身份。

您可以做甚麼：您可以遵循下一頁上的建議來幫助保護您的資料。您也可以使用上方提供的登記碼來登記加入由 TransUnion 為您提供的增補服務。

了解更多：有關如何保護您個人資料的更多資料載於下一頁。如果您有任何疑問或需要協助，請於星期一至星期五（不包括公眾假期）太平洋時間凌晨 5:00 至下午 5:00 致電 1-866-916-5125 聯絡 TransUnion。TransUnion 代表對此事件十分通曉，並可幫助您解答有關保護您資料的問題。

謹此問候

Children's Council of San Francisco（三藩市兒童委員會）
445 Church Street
San Francisco, CA 94114

您還可以採取哪些措施來進一步保護您的資料

檢視您的帳戶結單，並向執法部門舉報可疑活動：作為預防措施，我們建議您保持警惕，仔細檢視帳戶結單並密切監查免費信用報告是否有錯誤，並採取其他相應步驟（包括及時更改密碼）來保護帳戶。若您發現某個帳戶有任何可疑活動，應立即通知開設該帳戶的金融機構或公司，以獲得補救協助，或聯絡一間補救服務供應商。您亦應立即向相關執法機關、所在州的檢察總長及／或聯邦貿易委員會（FTC）舉報任何欺詐活動或任何疑似身份失竊事件。您還應聯絡當地的執法機關並報警。如有要求您向債權人提供副本以更正您的記錄，請取得報警回執副本。FTC 的聯絡資料如下：

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft。

信用報告副本：您每 12 個月可向三大信用報告機構各索取一份免費的信用報告副本，方法是造訪 <http://www.annualcreditreport.com/>、致電免付費電話 877-322-8228，或填寫年度信用報告申請表並郵寄至 Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348。您可以在 <https://www.annualcreditreport.com/cra/requestformfinal.pdf> 上打印出該申請表。您也可以聯絡以下三間國家級信用報告機構之一：

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com。
- *Experian*, P.O. Box 9701, Allen, TX 75013, 1-888-397-3742, www.experian.com。
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com。

防欺詐警訊：您可以在信用報告上設立兩種一般的防欺詐警訊——初始警訊和延時警訊。您可能想要考慮在您的信用報告上設立其中一種或兩種防欺詐警訊。初始防欺詐警訊為免費提供，並會在您的信用檔案中留存至少 90 天。該警訊會將您的報告中可能發生的欺詐活動通知債權人，並要求債權人在以您的名義開設任何帳戶之前聯絡您。如果您是身分已失竊的受害人並提供相應的證明文件，便可以在您的信用報告上設立延時警訊。延時的防欺詐警訊亦免費提供，並會在您的信用報告中留存七年。要在您的信用報告上設立防欺詐警訊，請聯絡上述三間信用報告機構之一。更多資料請瀏覽 <http://www.annualcreditreport.com>。軍人亦可在服役期間於其信用報告上設立現役軍人防欺詐警訊。現役軍人防欺詐警訊為期一年，並可在您服役期間續期。

信用或安全凍結：依據美國法律，您有權在您的信用檔案上設立為期長達一年的信用凍結（亦稱為安全凍結），但不必支付費用。此項凍結將防範任何人在不使用您啟動凍結時簽發給您的 PIN 碼情況下，以您的名義開設新的信貸帳戶。安全凍結旨在防止潛在的債權人不經您同意就存取您的信用報告。所以，使用安全凍結可能會妨礙或拖延您獲得信貸的能力。

您必須分別在各信用報告機構為您的信用檔案設立安全凍結。設立或解除安全凍結無需支付手續費。有關如何設立安全凍結的資料和指示，請聯絡上述任一信用報告機構或 FTC。為設立安全凍結，您可能需要向消費者報告機構提供可識別您身份的資料，包括您的全名、社會保障號碼、出生日期、目前和先前的地址、州簽發的身份證副本，以及最近一次水電費賬單、銀行結單或保險結單。收到您的凍結申請後，每間信用機構會為您提供獨一的 PIN 碼或密碼。請將該 PIN 碼或密碼保存在安全之處，因為日後若您選擇解除凍結則要用到它。

在您要求信用機構暫時解除或完全解除凍結之前，凍結依然有效。如果是在網上或致電提出申請，信用機構必須在一小時內解除信用凍結。如果是透過郵寄提出申請，則機構必須在收到您的申請後三個工作日內解除凍結。

IRS 身份保護 PIN 碼：您可以向美國國稅局（IRS）索取身份保護 PIN 碼（IP PIN），以防止他人使用您的社會保障號碼報稅。IP PIN 僅限您和 IRS 知曉，在您提交電子或紙質報稅單時，可用以幫助 IRS 驗證您的身份。您可以在此處了解詳情並取得您的 IP PIN：<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>。

依據《公平信用報告法案》（FCRA），您亦享有若干權利：這些權利包括了解您檔案中有甚麼資料、質疑不齊全或不準確的資料、要求消費者報告機構更正或刪除不準確、不完整或無從驗證資料的權利。有關 FCRA 的更多資料，以及 FCRA 項下您享有的權利，請瀏覽：

http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf。

其他免費的資源：您可以向消費者報告機構、FTC 或您所在州的檢察總長索取有關欺詐警訊、安全凍結，以及您可採取哪些身份防盜步驟的資訊。您可以向當地執法機關舉報疑似身份失竊事件，包括向 FTC 或您所在州的檢察總長舉報。

其他資料：

加州：加州檢察總長可通過以下方式聯絡：1300 I Street, Sacramento, CA 95814; 800-952-5225; www.oag.ca.gov/privacy

愛荷華州：愛荷華州檢察總長可通過以下方式聯絡：1305 E. Walnut St., Des Moines, IA 50319; 888-777-4590; www.iowaattorneygeneral.gov

馬里蘭州：馬里蘭州檢察總長可通過以下方式聯絡：200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us 或 IDTheft@oag.state.md.us

俄勒岡州：俄勒岡州檢察總長可通過以下方式聯絡：1162 Court St., NE, Salem, OR 97301; 877-877-9392; www.doj.state.or.us/consumer-protection

紐約州：紐約州檢察總長可通過以下方式聯絡：Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

北卡羅萊納州：北卡羅萊納州檢察總長辦公廳消費者保護處可通過以下方式聯絡：9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM（北卡羅萊納州境內免付費專線）；919-716-6000; www.ncdoj.gov

華盛頓特區：華盛頓特區檢察總長可通過以下方式聯絡：400 S 6th Street, NW Washington, DC 20001 www.oag.dc.gov 1-202-727-3400