20045

KIPP COLORADO SCHOOLS

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a recent data incident ("Incident") affecting KIPP Colorado Schools ("KIPP") that may have resulted in the disclosure of some of your personally identifiable information ("PII"). We take the privacy and protection of your personal information very seriously, and sincerely apologize for any inconvenience this Incident may cause. This letter contains information about the Incident and steps you can take to help protect your information.

In August 2019, KIPP experienced a business email compromise whereupon an unauthorized individual attempted to commit wire fraud against KIPP. The attempt was unsuccessful, and our internal IT team immediately reviewed audit logs to determine the nature and extent of the compromise. KIPP also engaged a third party vendor to determine what KIPP employee or student information may have been viewed or accessed by a threat actor. A total of five email accounts were compromised. Contained within the email accounts may have included your name, address, and Social Security number. Apart from these limited data elements, your credit card, financial account, or banking information were not involved in this incident.

At this time, we have no reason to believe that any personal information has been misused as a result of this Incident. However, for purposes of full disclosure, we feel it important to inform you that limited information may have been viewed by unauthorized individuals as a result of this Incident.

KIPP is committed to ensuring the security of all personal information in our control. As always, we recommend that you continue to join us in remaining vigilant to protect your personal information. As an added precaution, we have secured the services of Kroll, a leading global provider of risk solutions, to provide you with complimentary identity monitoring services. Information about the services being provided by Kroll, along with additional information about how to help protect yourself, is included in the materials attached to this letter.

Please review the enclosed "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission ("FTC") regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Please continue to remain vigilant, and carefully monitor your mail and credit reports for any suspect activity, and report any incident of identity theft to your local law enforcement, Attorney General, and the FTC.

Please know that safeguarding your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause to you and your family. If you have any questions, please do not hesitate to contact us at 1-???-???-????, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding some U.S. holidays.

Sincerely,

Tomi Amos
Chief Executive Officer
KIPP Colorado Schools

ELN-6788

KIPP COLORADO SCHOOLS

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Estimado/Estimada <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

El propósito de la presente es informarle de un incidente de datos reciente (el "Incidente") que afecta a las Escuelas KIPP Colorado ("KIPP") que puede haber resultado en la divulgación de alguna información de carácter personal ("PII") suya. Consideramos muy seriamente la privacidad y la protección de su información personal y sinceramente queremos disculparnos por cualquier inconveniente que este incidente pueda ocasionar. Esta carta contiene información sobre el "Incidente" y los pasos que usted puede dar para ayudar a proteger su información.

En agosto de 2019, el correo electrónico de KIPP se vio comprometido cuando un individuo no autorizado intentó cometer fraude electrónico contra KIPP. El intentó fracasó y nuestro equipo de TI interno revisó inmediatamente los registros de auditoría para determinar la naturaleza y extensión de lo que se había visto comprometido. KIPP también contrató a un proveedor independiente para determinar qué parte de la información de los empleados o alumnos de KIPP podía haber sido vista o accedida por un actor amenazante. Un total de cinco cuentas de correo electrónico se vieron comprometidas. Las cuentas de correo electrónico podrían haber incluido el nombre, dirección y el número de Seguro Social de usted. Aparte de estos elementos de datos limitados, la tarjeta de crédito, la cuenta financiera o la información bancaria de usted no se vieron comprometidas en este incidente.

En este momento, no tenemos razón para creer que haya sido mal utilizada alguna información personal como resultado de este incidente. Sin embargo, para propósitos de una total divulgación, creemos que es importante informarle que la información limitada puede haber sido vista por individuos no autorizados como resultado de este "Incidente".

KIPP tiene el compromiso de garantizar la seguridad de la información personal bajo nuestro control. Como siempre, le recomendamos que con nosotros siga vigilante para proteger su información personal. Como precaución adicional, hemos contratado los servicios de Kroll, un proveedor mundial líder en soluciones de riesgos, para darle a usted servicios de vigilancia de identidad en forma gratuita. La información sobre los servicios de Kroll, junto con información adicional sobre cómo audar a protegerse usted mismo, se incluye con los materiales adjuntos a esta carta.

Sírvase revisar la sección "Información adicional importante" que se incluye con esta carta. Esta sección describe los pasos adicionales que puede dar para protegerse usted mismo, así como las recomendaciones de la Comisión Federal de Comercio (FTC) respecto a la protección contra el robo de identidad y los detalles sobre cómo establecer un alerta de fraude o bloqueo de seguridad de su archivo de crédito. Le rogamos que permanezca vigilante y vigile cuidadosamente su correo e informes crediticios por si hay alguna actividad sospechosa, y reporte cualquier incidente de robo de identidad a cualquier agente del orden público local, al fiscal general y la FTC.

Tenga presente que la protección de su información personal es una prioridad principal y sinceramente lamentamos cualquier preocupación o inconveniente que este asunto pueda haberle causado a usted y su familia. Si tiene alguna pregunta, no dude en comunicarse con nosotros al 1-???-???-????, de lunes a viernes de 9:00 a.m. a 6:30 p.m., hora oficial del Este, menos los días feriados de EE.UU.

Atentamente,

Tomi Amos
Chief Executive Officer
Escuelas KIPP Colorado

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of District of Columbia: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202)442-9828 https://oag.dc.gov/consumer-protection

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Información adicional importante

Para los residentes de Hawái, Michigan, Missouri, Virginia, Vermont y Carolina del Norte: La ley estatal recomienda, para permanecer vigilante respecto a incidentes de fraude y robo de identidad, que revise los estados de cuenta de las tarjetas de crédito y vigile su informe crediticio por si aparece alguna actividad no autorizada.

Para residentes de Illinois, Iowa, Maryland, Missouri, Carolina del Norte y Virginia Occidental: La ley estatal exige que le informemos que puede obtener una copia de su informe crediticio, sin costo, sospeche usted o no de actividad no autorizada en su cuenta. Puede obtener una copia gratuita de su informe crediticio de cada una de las tres agencias nacionales de informe crediticio. Para pedir su informe crediticio gratuito, sírvase visitar www.annualcreditreport.com, o llame sin costo al 1-877-322-8228. También puede pedir su informe crediticio anual gratuito por correo enviando un Formulario de pedido de informe crediticio anual (disponible en https://www.consumer.ftc.gov/ articles/0155-free-credit-reports) a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Para los residentes de Iowa:

La ley estatal le aconseja que informe cualquier sospecha de robo de identidad a los agentes del orden público o al fiscal general.

Para los residentes de Oregón:

La ley estatal le aconseja que informe cualquier sospecha de robo de identidad a los agentes del orden público, al fiscal general y la Comisión Federal de Comercio.

Para los residentes de Maryland, Rhode Island, Illinois, Nueva y Carolina del Norte: Usted puede obtener información de las Oficinas del Fiscal General y de la Comisión Federal de Comercio de Maryland y Carolina del Norte sobre alertas de fraude, bloqueos de seguridad y los pasos que puede tomar para prevenir el robo de identidad.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Para los residentes de Massachusetts: La ley estatal exige que se le informe sobre su derecho a obtener un informe policial en caso usted haya sido víctima de robo de identidad.

Para los residentes del Distrito de Columbia: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202)442-9828 https://oag.dc.gov/consumer-protection

Para los residentes de todos los estados:

Alertas de fraude: Usted puede establecer alertas de fraude en las tres agencias crediticias por teléfono y por internet, con Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); o Experian (https://www. experian.com/fraud/center.html). Una alerta de fraude informa a los acreedores que sigan ciertos procedimientos, incluso el comunicarse con usted, antes de abrir cualquier nueva cuenta o cambiar una cuenta existente. Por esta razón, establecer una alerta de fraude puede protegerle, pero también demorarlo cuando usted solicite un crédito. Al 21 de septiembre de 2018, las alertas de fraude iniciales duran un año. Las víctimas de robo de identidad también pueden obtener una extensión de la alerta de fraude hasta por siete años. Los números de teléfono de las tres agencias crediticias están al final de esta página.

Vigilancia: Usted siempre debería permanecer vigilante de sus cuentas para detectar actividades sospechosas o inusuales.

Bloqueo de seguridad: Usted también tiene el derecho de establecer un bloqueo de seguridad en su informe crediticio. Un bloqueo de seguridad tiene el propósito de prevenir que créditos, préstamos y servicios sean aprobados en su nombre sin su consentimiento Para establecer un bloqueo de seguridad en su informe crediticio, usted deberá solicitarlo a cada agencia de informe crediticio. Puede hacer la solicitud por correo certificado, correo de un día para otro, correo regular con estampillas o siguiendo las instrucciones que aparecen en los sitios web indicados abajo. Debe incluirse la información siguiente al pedir un bloqueo de seguridad (tome nota de que si usted pide un informe crediticio para su cónyuge o una persona menor de 16 años de edad, también deberá dar la información de ellos): (1) Nombre, inicial del segundo nombre y apellido, con cualquier sufijo; (2) Número de seguro social; (3) fecha de nacimiento; (4) dirección actual y cualquier dirección previa en los últimos cinco años y (5) cualquier informe de incidente o queja de una agencia del orden público o del Registro de vehículos automotores. La solicitud debe también incluir una copia de una tarjeta de identificación emitida por el gobierno y una copia de una factura reciente de servicios públicos o un estado reciente de cuenta bancaria o de seguros. Es fundamental que cada copia sea legible, muestre su nombre y dirección postal actual, y la fecha de emisión. Al 21 de septiembre de 2018, es gratis establecer y retirar un bloqueo de seguridad. También puede establecer un bloqueo de seguridad para niños menores de 16 años de edad. Puede obtener un bloque de seguridad gratuito comunicándose con una o más de las agencias nacionales de informes del consumidor:

Bloqueo de seguridad de Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Bloqueo de seguridad de Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

Para obtener más información puede comunicarse con la Comisión Federal de Comercio, cuya información está abajo.

Activate Your Monitoring Services

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 **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **May 10, 2021** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

Active sus servicios de vigilancia

Para ayudar a calmar las preocupaciones y restablecer la confianza después de sucedido este incidente, hemos contratado los servicios de Kroll para darle servicios de vigilancia de identidad de manera gratuita para usted por un año. Kroll es un líder mundial en mitigación y respuesta a riesgos. Su equipo tiene amplia experiencia en ayudar a personas que han sufrido una exposición involuntaria de sus datos confidenciales. Los servicios de vigilancia de identidad incluyen vigilancia de crédito, consulta sobre fraude y recuperación de la identidad.

Visite **https://enroll.idheadquarters.com** para activar y aprovechar sus servicios de vigilancia de identidad.
*Tiene hasta el **10 de mayo de 2021** para activar sus servicios de vigilancia de identidad.*
Número de miembro: **<<Member ID>>**

Kroll | A Division of DUFF&PHELPS

APROVECHE LOS SERVICIOS DE VIGILANCIA DE IDENTIDAD

Se le ha dado acceso a usted a los siguientes servicios de Kroll:

Vigilancia de crédito por parte de una sola agencia

Usted recibirá alertas cuando haya cambios en sus datos de crédito. Por ejemplo, cuando se solicite una nueva línea de crédito en su nombre. Si usted no reconoce la actividad, tendrá la opción de llamar al especialista en fraudes de Kroll quien podrá ayudarle a determinar si se trata de un indicador de robo de identidad.

Consulta sobre fraude

Usted tendrá acceso ilimitado a consultar con un especialista en fraudes de Kroll. El apoyo incluye mostrarle las maneras más eficaces de proteger su identidad, explicarle sus derechos y protecciones bajo la ley, ayudarle con los alertas de fraude, e interpretar como se accedió y utilizó la información personal, incluso la investigación de actividad sospechosa que podría estar asociada a un evento de robo de identidad.

Recuperación de la identidad

Si usted es víctima de robo de identidad, un investigador autorizado con experiencia de Kroll trabajará en su nombre para resolver los problemas relacionados. Tendrá acceso a un investigador dedicado que comprende sus problemas y hará la mayor parte del trabajo por usted. Su investigador podrá profundizar para descubrir el alcance del robo de identidad.

El sitio web de activación de Kroll es compatible solamente con la versión actual o una versión previa de Chrome, Firefox, Safari y Edge. Para recibir los servicios crediticios, usted debe ser mayor de 18 años de edad y tener un crédito establecido en EE. UU., tener un número de Seguro social en su nombre y una dirección de residencia en EE. UU. en su archivo crediticio.

KIPP COLORADO SCHOOLS

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a recent data incident ("Incident") affecting KIPP Colorado Schools ("KIPP") that may have resulted in the disclosure of some of your personally identifiable information ("PII"). We take the privacy and protection of your personal information very seriously, and sincerely apologize for any inconvenience this Incident may cause. This letter contains information about the Incident and steps you can take to help protect your information.

In August 2019, KIPP experienced a business email compromise whereupon an unauthorized individual attempted to commit wire fraud against KIPP. The attempt was unsuccessful, and our internal IT team immediately reviewed audit logs to determine the nature and extent of the compromise. KIPP also engaged a third party vendor to determine what KIPP employee or student information may have been viewed or accessed by a threat actor. A total of five email accounts were compromised. Contained within the email accounts may have included your name, address, and student ID number. Apart from these limited data elements, your Social Security number, credit card, financial account, or banking information were not involved in this incident.

At this time, we have no reason to believe that any personal information has been misused as a result of this Incident. However, for purposes of full disclosure, we feel it important to inform you that limited information may have been viewed by unauthorized individuals as a result of this Incident.

KIPP is committed to ensuring the security of all personal information in our control. As always, we recommend that you continue to join us in remaining vigilant to protect your personal information.

Please review the enclosed "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission ("FTC") regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Please continue to remain vigilant, and carefully monitor your mail and credit reports for any suspect activity, and report any incident of identity theft to your local law enforcement, Attorney General, and the FTC.

Please know that safeguarding your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause to you and your family. If you have any questions, please do not hesitate to contact us at 1-???-???-????, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding some U.S. holidays.

Sincerely,

Tomi Amos
Chief Executive Officer
KIPP Colorado Schools

KIPP COLORADO SCHOOLS

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Estimado/Estimada <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

El propósito de la presente es informarle de un incidente de datos reciente (el "Incidente") que afecta a las Escuelas KIPP Colorado ("KIPP") y que puede haber resultado en la divulgación de alguna información de carácter personal ("PII") suya. Consideramos muy seriamente la privacidad y la protección de su información personal y sinceramente queremos disculparnos por cualquier inconveniente que este incidente pueda ocasionar. Esta carta contiene información sobre el "Incidente" y los pasos que usted puede dar para ayudar a proteger su información.

En agosto de 2019, el correo electrónico de KIPP se vio comprometido cuando un individuo no autorizado intentó cometer fraude electrónico contra KIPP. El intentó fracasó y nuestro equipo de TI interno revisó inmediatamente los registros de auditoría para determinar la naturaleza y extensión de lo que se había visto comprometido. KIPP también contrató a un proveedor independiente para determinar qué parte de la información de los empleados o alumnos de KIPP podía haber sido vista o accedida por un actor amenazante. Un total de cinco cuentas de correo electrónico se vieron comprometidas. Las cuentas de correo electrónico podrían haber incluido el nombre y dirección de usted y el número de identificación del alumno. Aparte de estos elementos de datos limitados, el número de Seguro Social, la tarjeta de crédito ni la información bancaria de usted no se vieron comprometidas en este incidente.

En este momento, no tenemos razón para creer que haya sido mal utilizada alguna información personal como resultado de este incidente. Sin embargo, para propósitos de una total divulgación, creemos que es importante informarle que la información limitada puede haber sido vista por individuos no autorizados como resultado de este "Incidente".

KIPP tiene el compromiso de garantizar la seguridad de la información personal bajo nuestro control. Como siempre, le recomendamos que con nosotros siga vigilante para proteger su información personal.

Sírvase revisar la sección "Información adicional importante" que se incluye con esta carta. Esta sección describe los pasos adicionales que puede dar para protegerse usted mismo, así como las recomendaciones de la Comisión Federal de Comercio (FTC) respecto a la protección contra el robo de identidad y los detalles sobre cómo establecer una alerta de fraude o bloqueo de seguridad de su archivo de crédito. Le rogamos que permanezca vigilante y vigile cuidadosamente su correo e informes crediticios por si hay alguna actividad sospechosa, y reporte cualquier incidente de robo de identidad a su agencia del orden público local, al fiscal general y la FTC.

Tenga presente que la protección de su información personal es una prioridad principal y sinceramente lamentamos cualquier preocupación o inconveniente que este asunto pueda haberle causado a usted y su familia. Si tiene alguna pregunta, no dude en comunicarse con nosotros al 1-???-???-????, de lunes a viernes de 9:00 a.m. a 6:30 p.m., hora oficial del Este, menos los días feriados de EE.UU.

Atentamente,

Tomi Amos
Chief Executive Officer
Escuelas KIPP Colorado

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of District of Columbia: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202)442-9828 https://oag.dc.gov/consumer-protection

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Información adicional importante

Para los residentes de Hawái, Michigan, Missouri, Virginia, Vermont y Carolina del Norte: La ley estatal recomienda, para permanecer vigilante respecto a incidentes de fraude y robo de identidad, que revise los estados de cuenta de las tarjetas de crédito y vigile su informe crediticio por si aparece alguna actividad no autorizada.

Para residentes de Illinois, Iowa, Maryland, Missouri, Carolina del Norte y Virginia Occidental: La ley estatal exige que le informemos que puede obtener una copia de su informe crediticio, sin costo, sospeche usted o no de actividad no autorizada en su cuenta. Puede obtener una copia gratuita de su informe crediticio de cada una de las tres agencias nacionales de informe crediticio. Para pedir su informe crediticio gratuito, sírvase visitar www.annualcreditreport.com, o llame sin costo al 1-877-322-8228. También puede pedir su informe crediticio anual gratuito por correo enviando un Formulario de pedido de informe crediticio anual (disponible en https://www.consumer.ftc.gov/ articles/0155-free-credit-reports) a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Para los residentes de Iowa:

La ley estatal le aconseja que informe cualquier sospecha de robo de identidad a los agentes del orden público o al fiscal general.

Para los residentes de Oregón:

La ley estatal le aconseja que informe cualquier sospecha de robo de identidad a los agentes del orden público, al fiscal general y la Comisión Federal de Comercio.

Para los residentes de Maryland, Rhode Island, Illinois, Nueva y Carolina del Norte: Usted puede obtener información de las Oficinas del Fiscal General y de la Comisión Federal de Comercio de Maryland y Carolina del Norte sobre alertas de fraude, bloqueos de seguridad y los pasos que puede tomar para prevenir el robo de identidad.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Para los residentes de Massachusetts: La ley estatal exige que se le informe sobre su derecho a obtener un informe policial en caso usted haya sido víctima de robo de identidad.

Para los residentes del Distrito de Columbia: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202)442-9828 https://oag.dc.gov/consumer-protection

Para los residentes de todos los estados:

Alertas de fraude: Usted puede establecer alertas de fraude en las tres agencias crediticias por teléfono y por internet, con Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); o Experian (https://www. experian.com/fraud/center.html). Una alerta de fraude informa a los acreedores que sigan ciertos procedimientos, incluso el comunicarse con usted, antes de abrir cualquier nueva cuenta o cambiar una cuenta existente. Por esta razón, establecer una alerta de fraude puede protegerle, pero también demorarlo cuando usted solicite un crédito. Al 21 de septiembre de 2018, las alertas de fraude iniciales duran un año. Las víctimas de robo de identidad también pueden obtener una extensión de la alerta de fraude hasta por siete años. Los números de teléfono de las tres agencias crediticias están al final de esta página.

Vigilancia: Usted siempre debería permanecer vigilante de sus cuentas para detectar actividades sospechosas o inusuales.

Bloqueo de seguridad: Usted también tiene el derecho de establecer un bloqueo de seguridad en su informe crediticio. Un bloqueo de seguridad tiene el propósito de prevenir que créditos, préstamos y servicios sean aprobados en su nombre sin su consentimiento Para establecer un bloqueo de seguridad en su informe crediticio, usted deberá solicitarlo a cada agencia de informe crediticio. Puede hacer la solicitud por correo certificado, correo de un día para otro, correo regular con estampillas o siguiendo las instrucciones que aparecen en los sitios web indicados abajo. Debe incluirse la información siguiente al pedir un bloqueo de seguridad (tome nota de que si usted pide un informe crediticio para su cónyuge o una persona menor de 16 años de edad, también deberá dar la información de ellos): (1) Nombre, inicial del segundo nombre y apellido, con cualquier sufijo; (2) Número de seguro social; (3) fecha de nacimiento; (4) dirección actual y cualquier dirección previa en los últimos cinco años y (5) cualquier informe de incidente o queja de una agencia del orden público o del Registro de vehículos automotores. La solicitud debe también incluir una copia de una tarjeta de identificación emitida por el gobierno y una copia de una factura reciente de servicios públicos o un estado reciente de cuenta bancaria o de seguros. Es fundamental que cada copia sea legible, muestre su nombre y dirección postal actual, y la fecha de emisión. Al 21 de septiembre de 2018, es gratis establecer y retirar un bloqueo de seguridad. También puede establecer un bloqueo de seguridad para niños menores de 16 años de edad. Puede obtener un bloque de seguridad gratuito comunicándose con una o más de las agencias nacionales de informes del consumidor:

Bloqueo de seguridad de Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Bloqueo de seguridad de Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

Para obtener más información puede comunicarse con la Comisión Federal de Comercio, cuya información está abajo.

KIPP COLORADO SCHOOLS

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a recent data incident ("Incident") affecting KIPP Colorado Schools ("KIPP") that may have resulted in the disclosure of some of your personally identifiable information ("PII"). We take the privacy and protection of your personal information very seriously, and sincerely apologize for any inconvenience this Incident may cause. This letter contains information about the Incident and steps you can take to help protect your information.

In August 2019, KIPP experienced a business email compromise whereupon an unauthorized individual attempted to commit wire fraud against KIPP. The attempt was unsuccessful, and our internal IT team immediately reviewed audit logs to determine the nature and extent of the compromise. KIPP also engaged a third party vendor to determine what KIPP employee or student information may have been viewed or accessed by a threat actor. A total of five email accounts were compromised. Contained within the email accounts may have included your name, address, and financial account number. Apart from these limited data elements, your Social Security number was not involved in this incident.

At this time, we have no reason to believe that any personal information has been misused as a result of this Incident. However, for purposes of full disclosure, we feel it important to inform you that limited information may have been viewed by unauthorized individuals as a result of this Incident.

KIPP is committed to ensuring the security of all personal information in our control. As always, we recommend that you continue to join us in remaining vigilant to protect your personal information.

Please review the enclosed "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission ("FTC") regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Please continue to remain vigilant, and carefully monitor your mail and credit reports for any suspect activity, and report any incident of identity theft to your local law enforcement, Attorney General, and the FTC.

Please know that safeguarding your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause to you and your family. If you have any questions, please do not hesitate to contact us at 1-???-???-????, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding some U.S. holidays.

Sincerely,

Tomi Amos
Chief Executive Officer
KIPP Colorado Schools

KIPP COLORADO SCHOOLS

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Estimado/Estimada <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

El propósito de la presente es informarle de un incidente de datos reciente (el "Incidente") que afecta a las Escuelas KIPP Colorado ("KIPP") que puede haber resultado en la divulgación de alguna información de carácter personal ("PII") suya. Consideramos muy seriamente la privacidad y la protección de su información personal y sinceramente queremos disculparnos por cualquier inconveniente que este incidente pueda ocasionar. Esta carta contiene información sobre el "Incidente" y los pasos que usted puede dar para ayudar a proteger su información.

En agosto de 2019, el correo electrónico de KIPP se vio comprometido cuando un individuo no autorizado intentó cometer fraude electrónico contra KIPP. El intentó fracasó y nuestro equipo de TI interno revisó inmediatamente los registros de auditoría para determinar la naturaleza y extensión de lo que se había visto comprometido. KIPP también contrató a un proveedor independiente para determinar qué parte de la información de los empleados o alumnos de KIPP podía haber sido vista o accedida por un actor amenazante. Un total de cinco cuentas de correo electrónico se vieron comprometidas. Las cuentas de correo electrónico podrían haber incluido el nombre, dirección y número de cuenta financiera de usted. Aparte de esos elementos de datos limitados, el número de Seguro Social de usted no se vio comprometido en este incidente.

En este momento, no tenemos razón para creer que haya sido mal utilizada alguna información personal como resultado de este incidente. Sin embargo, para propósitos de una total divulgación, creemos que es importante informarle que la información limitada puede haber sido vista por individuos no autorizados como resultado de este "Incidente".

KIPP tiene el compromiso de garantizar la seguridad de la información personal bajo nuestro control. Como siempre, le recomendamos que con nosotros siga vigilante para proteger su información personal.

Sírvase revisar la sección "Información adicional importante" que se incluye con esta carta. Esta sección describe los pasos adicionales que puede dar para protegerse usted mismo, así como las recomendaciones de la Comisión Federal de Comercio (FTC) respecto a la protección contra el robo de identidad y los detalles sobre cómo establecer un alerta de fraude o bloqueo de seguridad de su archivo de crédito. Le rogamos que permanezca vigilante y vigile cuidadosamente su correo e informes crediticios por si hay alguna actividad sospechosa, y reporte cualquier incidente de robo de identidad a cualquier agente del orden público local, al fiscal general y la FTC.

Tenga presente que la protección de su información personal es una prioridad principal y sinceramente lamentamos cualquier preocupación o inconveniente que este asunto pueda haberle causado a usted y su familia. Si tiene alguna pregunta, no dude en comunicarse con nosotros al 1-???-???-????, de lunes a viernes de 9:00 a.m. a 6:30 p.m., hora oficial del Este, menos los días feriados de EE.UU.

Atentamente,

Tomi Amos
Chief Executive Officer
Escuelas KIPP Colorado

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of District of Columbia: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202)442-9828 https://oag.dc.gov/consumer-protection

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Información adicional importante

Para los residentes de Hawái, Michigan, Missouri, Virginia, Vermont y Carolina del Norte: La ley estatal recomienda, para permanecer vigilante respecto a incidentes de fraude y robo de identidad, que revise los estados de cuenta de las tarjetas de crédito y vigile su informe crediticio por si aparece alguna actividad no autorizada.

Para residentes de Illinois, Iowa, Maryland, Missouri, Carolina del Norte y Virginia Occidental: La ley estatal exige que le informemos que puede obtener una copia de su informe crediticio, sin costo, sospeche usted o no de actividad no autorizada en su cuenta. Puede obtener una copia gratuita de su informe crediticio de cada una de las tres agencias nacionales de informe crediticio. Para pedir su informe crediticio gratuito, sírvase visitar www.annualcreditreport.com, o llame sin costo al 1-877-322-8228. También puede pedir su informe crediticio anual gratuito por correo enviando un Formulario de pedido de informe crediticio anual (disponible en https://www.consumer.ftc.gov/ articles/0155-free-credit-reports) a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Para los residentes de Iowa:

La ley estatal le aconseja que informe cualquier sospecha de robo de identidad a los agentes del orden público o al fiscal general.

Para los residentes de Oregón:

La ley estatal le aconseja que informe cualquier sospecha de robo de identidad a los agentes del orden público, al fiscal general y la Comisión Federal de Comercio.

Para los residentes de Maryland, Rhode Island, Illinois, Nueva y Carolina del Norte: Usted puede obtener información de las Oficinas del Fiscal General y de la Comisión Federal de Comercio de Maryland y Carolina del Norte sobre alertas de fraude, bloqueos de seguridad y los pasos que puede tomar para prevenir el robo de identidad.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Para los residentes de Massachusetts: La ley estatal exige que se le informe sobre su derecho a obtener un informe policial en caso usted haya sido víctima de robo de identidad.

Para los residentes del Distrito de Columbia: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202)442-9828 https://oag.dc.gov/consumer-protection

Para los residentes de todos los estados:

Alertas de fraude: Usted puede establecer alertas de fraude en las tres agencias crediticias por teléfono y por internet, con Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); o Experian (https://www. experian.com/fraud/center.html). Una alerta de fraude informa a los acreedores que sigan ciertos procedimientos, incluso el comunicarse con usted, antes de abrir cualquier nueva cuenta o cambiar una cuenta existente. Por esta razón, establecer una alerta de fraude puede protegerle, pero también demorarlo cuando usted solicite un crédito. Al 21 de septiembre de 2018, las alertas de fraude iniciales duran un año. Las víctimas de robo de identidad también pueden obtener una extensión de la alerta de fraude hasta por siete años. Los números de teléfono de las tres agencias crediticias están al final de esta página.

Vigilancia: Usted siempre debería permanecer vigilante de sus cuentas para detectar actividades sospechosas o inusuales.

Bloqueo de seguridad: Usted también tiene el derecho de establecer un bloqueo de seguridad en su informe crediticio. Un bloqueo de seguridad tiene el propósito de prevenir que créditos, préstamos y servicios sean aprobados en su nombre sin su consentimiento Para establecer un bloqueo de seguridad en su informe crediticio, usted deberá solicitarlo a cada agencia de informe crediticio. Puede hacer la solicitud por correo certificado, correo de un día para otro, correo regular con estampillas o siguiendo las instrucciones que aparecen en los sitios web indicados abajo. Debe incluirse la información siguiente al pedir un bloqueo de seguridad (tome nota de que si usted pide un informe crediticio para su cónyuge o una persona menor de 16 años de edad, también deberá dar la información de ellos): (1) Nombre, inicial del segundo nombre y apellido, con cualquier sufijo; (2) Número de seguro social; (3) fecha de nacimiento; (4) dirección actual y cualquier dirección previa en los últimos cinco años y (5) cualquier informe de incidente o queja de una agencia del orden público o del Registro de vehículos automotores. La solicitud debe también incluir una copia de una tarjeta de identificación emitida por el gobierno y una copia de una factura reciente de servicios públicos o un estado reciente de cuenta bancaria o de seguros. Es fundamental que cada copia sea legible, muestre su nombre y dirección postal actual, y la fecha de emisión. Al 21 de septiembre de 2018, es gratis establecer y retirar un bloqueo de seguridad. También puede establecer un bloqueo de seguridad para niños menores de 16 años de edad. Puede obtener un bloque de seguridad gratuito comunicándose con una o más de las agencias nacionales de informes del consumidor:

Bloqueo de seguridad de Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Bloqueo de seguridad de Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

Para obtener más información puede comunicarse con la Comisión Federal de Comercio, cuya información está abajo.