amerlux
A Delta Group Company

Return to IDX:
4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

April 22, 2024

RE: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

We recently discovered that Amerlux LLC, a subsidiary of Delta Electronics, Inc., ("Amerlux," "we," "us") was the victim of a ransomware attack that involved some of the personal information we hold about you. We are writing to explain what happened, how we have responded, and what you can do to protect your personal information.

1. **Here is what happened**:

On the morning of March 13, 2024, Amerlux's independent information technology ("IT") vendor discovered that a cybercriminal had launched an attack on Amerlux's computer servers. Amerlux's IT vendor discovered the attack at approximately 6:00 a.m. and immediately disconnected all devices from the Amerlux network, as well as contacted Ra Security Systems ("Ra Security"), a cybersecurity recovery and investigation firm, to investigate the incident.

Ra Security informed us that the incident began on approximately March 7, 2024 and ended on March 13, 2024 when Amerlux's IT vendor successfully disconnected all devices from the Amerlux network. According to Ra Security's investigation, as well as the investigation of Amerlux's IT security team, a well-known ransomware group was responsible for the attack. The cybercriminal encrypted Amerlux's computer servers with ransomware and was able to access certain files in our network.

Our initial understanding of the incident was that neither Amerlux employee nor customer information was affected by the ransomware attack; however, we continued our internal review of the data maintained on the affected servers. Regrettably, on March 28, 2024, we learned that the files potentially accessed by the cybercriminal included certain human resources data, such as W-2s of current and former Amerlux employees, as well as certain information that employees may have saved to their desktops and/or laptops and was then automatically backed up to the server. Ra Security informed us that the cybercriminal was able to exfiltrate at least some of this data. On this same day, Amerlux contacted and engaged cybersecurity legal counsel to coordinate efforts with our IT security team.

2. **How we responded:**

As explained above, on March 13th, immediately upon becoming aware of the ransomware attack, Amerlux's IT vendor immediately disconnected all devices from the Amerlux network and contacted Ra Security. On the same day, Amerlux instructed all employees to change their passwords to Amerlux systems.

Amerlux's IT security team continued to closely monitor its network and third-party hosted systems, such as Oracle and Workday, for unusual activity. Ra Security has confirmed that such systems remained secure during the attack and were not affected. Amerlux also promptly installed updated antivirus software on each computer.

We are notifying relevant state authorities of this cyberattack. While no business can be 100% secure, we are working with Ra Security to evaluate ways in which we can reduce the likelihood of a future cyberattack.

3. **Types of information involved:**

Based upon Ra Security's investigation, the cybercriminal's access to identifiable data was limited to a shared drive containing human resources data and data backups from employee desktops and laptops. While the types of information affected will vary by person, the personal information maintained in the affected files generally included the following: names; addresses; Social Security Numbers; salary data; bank account information for employees actively employed with Amerlux on or after January 1, 2021; and passport numbers backed up from images saved by employees on their work desktops and/or laptops.

4. **Protection of your information:**

We are providing written notice to all individuals that we have identified as having information potentially affected by this incident. Included with this notice is a "Reference Guide," which provides useful information regarding how to protect your identity, including obtaining copies of your credit report and implementing credit freezes. We encourage you to review the Reference Guide closely.

In addition, we are offering you twenty-four (24) months of identity theft protection services through IDX, a ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is July 22, 2024.

5. **For more information:**

Amerlux takes its obligation to protect the privacy and confidentiality of our employees' personal information very seriously and we deeply regret that this breach occurred. If you have any questions, you may contact Michele Edelstein by phone at 973-882-5010 ext. 375 or by email at medelstein@amerlux.com.

Sincerely,

Chuck Campagna
President & CEO
Amerlux, LLC

Reference Guide

Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. The payment card brands' policies provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

Order A Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and about fraud alerts and security freezes:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 2002 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)
- Social Security Card, pay stub, or W2
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Additional Information for Massachusetts Residents.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. There is no longer a fee for placing, lifting, and/or removing a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348

Experian Security Freeze P.O. Box 9554 Allen, TX 75013

Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

amerlux
A Delta Group Company

Return to IDX:
4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

Código de inscripción: <<XXXXXXXX>>

Para inscribirse, escanee el código QR a continuación:

SCAN ME

O visite:
https://app.idx.us/account-creation/protect

22 de Abril de 2024

Asunto: Aviso de filtración de datos

Estimado(a) <<First Name>> <<Last Name>>:

Recientemente descubrimos que Amerlux LLC, una subsidiaria de Delta Electronics, Inc., ("Amerlux", "nosotros", "nos") fue víctima de un ataque de ransomware (secuestro de datos) que involucró parte de la información personal que tenemos sobre usted. Le escribimos para explicarle lo que sucedió, qué medidas tomamos y qué puede hacer usted para proteger su información personal.

1. **Esto es lo que sucedió**:

La mañana del 13 de marzo de 2024, el proveedor independiente de tecnología de la información (information technology, "IT") de Amerlux descubrió que un ciberdelincuente había lanzado un ataque contra los servidores informáticos de Amerlux. El proveedor de IT de Amerlux descubrió el ataque aproximadamente a las 6.00 a. m. e inmediatamente desconectó todos los dispositivos de la red de Amerlux y se comunicó con Ra Security Systems ("Ra Security"), una empresa de recuperación e investigación de ciberseguridad, para investigar el incidente.

Ra Security nos informó que el incidente comenzó aproximadamente el 7 de marzo de 2024 y finalizó el 13 de marzo de 2024 cuando el proveedor de IT de Amerlux desconectó con éxito todos los dispositivos de la red de Amerlux. Según la investigación de Ra Security, así como la investigación del equipo de seguridad de IT de Amerlux, el responsable del ataque es un conocido grupo dedicado al secuestro de datos cibernéticos. El ciberdelincuente cifró los servidores informáticos de Amerlux y pudo acceder a ciertos archivos de nuestra red.

Nuestra comprensión inicial del incidente fue que ni la información de los empleados de Amerlux ni la de los clientes se vieron afectadas por el ataque de ransomware; sin embargo, continuamos nuestra revisión interna de los datos mantenidos en los servidores afectados. Lamentablemente, el 28 de marzo de 2024, descubrimos que los archivos a los que posiblemente haya accedido el ciberdelincuente incluían ciertos datos de recursos humanos, como los formularios W-2 de empleados actuales y anteriores de Amerlux, así como cierta información que los empleados puedan haber guardado en sus computadoras de escritorio o portátiles y que luego se respaldó automáticamente en el servidor. Ra Security nos informó que el ciberdelincuente pudo extraer al menos algunos de estos datos. Ese mismo día, Amerlux contactó y contrató asesoramiento legal en ciberseguridad para coordinar esfuerzos con nuestro equipo de seguridad informática.

2. **Qué medidas tomamos:**

Como se explicó anteriormente, el 13 de marzo, inmediatamente después de tomar conocimiento del ataque, el proveedor de IT de Amerlux desconectó inmediatamente todos los dispositivos de la red de Amerlux y se comunicó con Ra Security. El mismo día, Amerlux ordenó a todos los empleados que cambiaran sus contraseñas para los sistemas de Amerlux.

El equipo de seguridad de IT de Amerlux siguió supervisando atentamente su red y los sistemas alojados de terceros, como Oracle y Workday, para detectar cualquier actividad inusual. Ra Security ha confirmado que dichos sistemas se mantuvieron seguros durante el ataque y no se vieron afectados. Amerlux también instaló rápidamente programas antivirus actualizados en cada computadora. Estamos notificando sobre este ciberataque a las autoridades estatales pertinentes. Si bien ninguna empresa puede ser 100 % segura, estamos trabajando con Ra Security para evaluar formas en las que podamos reducir el riesgo de un futuro ciberataque.

3. **Tipos de información involucrada:**

Según la investigación de Ra Security, el acceso del ciberdelincuente a los datos identificables se limitó a una unidad compartida que contenía datos de recursos humanos y copias de seguridad de datos desde las computadoras de escritorio y portátiles de los empleados. Si bien los tipos de información afectados variarán según la persona, la información personal que se encontraba en los archivos afectados incluía lo siguiente: nombres, direcciones, números del Seguro Social, datos salariales, información de cuentas bancarias para empleados activos de Amerlux a partir del 1 de enero de 2021; y números de pasaporte respaldados por imágenes guardadas por empleados en sus computadoras de escritorio o portátiles.

4. **Protección de su información:**

Estamos enviando una notificación por escrito a todas las personas que hemos identificado como posiblemente afectadas por este incidente. Junto con este aviso se incluye una "Guía de referencia", que proporciona información útil sobre cómo proteger su identidad, incluida la obtención de copias de su informe crediticio y la implementación de bloqueos de créditos. Le recomendamos que revise atentamente la Guía de referencia.

Además, le ofrecemos veinticuatro (24) meses de servicios de protección contra robo de identidad a través de IDX, una empresa de ZeroFox, experta en servicios de filtración y recuperación de datos. Los servicios de protección de identidad de IDX incluyen lo siguiente: 24 meses de crédito y monitoreo CyberScan, una póliza de reembolso de seguro de $1,000,000 y servicios de recuperación de robo de identidad totalmente administrados. Con esta protección, IDX le ayudará a resolver problemas si su identidad se ve comprometida. Le recomendamos que se comunique con IDX si tiene alguna pregunta y que se inscriba en los servicios gratuitos de protección de identidad llamando al 1-800-939-4170, visitando https://app.idx.us/account-creation/protect o escaneando el código QR de la imagen e ingresando el código de inscripción proporcionado anteriormente. Los representantes de IDX están disponibles de lunes a viernes de 9.00 a. m. a 9.00 p. m., hora del Este. Tenga en cuenta que el plazo para inscribirse es 22 de Julio de 2024.

5. **Para obtener más información, lea lo siguiente:**

En Amerlux nos tomamos muy en serio nuestra responsabilidad de proteger la privacidad y confidencialidad de la información personal de nuestros empleados y lamentamos profundamente este incidente. Si tiene alguna pregunta, puede comunicarse con Michele Edelstein por teléfono al 973-882-5010, ext. 375 o por correo electrónico en medelstein@amerlux.com.

Atentamente.

Chuck Campagna
Presidente y Director Ejecutivo
Amerlux, LLC

Guía de referencia

Revise sus estados de cuenta. Le recomendamos que permanezca atento revisando sus estados de cuenta. Si cree que hay un cargo no autorizado en su tarjeta, comuníquese con su institución financiera o emisor de la tarjeta de inmediato. Las políticas de las marcas de tarjetas de pago establecen que los titulares de tarjetas no tienen ninguna responsabilidad por los cargos no autorizados que se reporten de manera oportuna. Comuníquese con la marca de su tarjeta o con el banco emisor para obtener más información sobre la política que se aplica en su caso.

Solicite un informe de crédito gratis. Usted tiene derecho, en virtud de la ley de los EE. UU., a un informe de crédito gratuito anual de cada una de las tres agencias nacionales de informes de crédito del consumidor. Para solicitar su informe de crédito gratis, visite www.annualcreditreport.com, llame gratis al 1-877-322-8228 o complete el Formulario de Solicitud de Informe de Crédito Anual en el sitio web de la Comisión Federal de Comercio de los EE. UU. ("FTC") en www.consumer.ftc.gov y envíelo por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Las tres agencias de informes de crédito del consumidor a nivel nacional proporcionan informes de crédito anuales gratuitos solo a través del sitio web, el número gratuito o el formulario de solicitud.

Cuando reciba su informe de crédito, revíselo detenidamente. Busque cuentas que no abrió. Busque la sección "Consultas" para ver los nombres de los acreedores a los que no ha solicitado crédito. Algunas empresas facturan con nombres distintos a los de su tienda o nombre comercial. La agencia de informes de crédito del consumidor podrá decirle cuándo es ese el caso. Consulte la sección "Información personal" para ver si hay imprecisiones en su información (como la dirección particular y el número de Seguro Social). Si ve algo que no comprende, llame a la agencia de informes de crédito del consumidor al número de teléfono que figura en el informe. Los errores en esta información pueden ser una señal de advertencia de un posible robo de identidad. Debe notificar a las agencias de informes de crédito del consumidor cualquier inexactitud en su informe, ya sea debido a un error o fraude, lo antes posible para que la información pueda investigarse y, si se descubre que es un error, corregirse. Si hay cuentas o cargos que usted no autorizó, notifique de inmediato a la agencia de informes de crédito del consumidor correspondiente por teléfono y por escrito. El personal de la agencia de informes de crédito del consumidor revisará su informe con usted. Si la información no puede explicarse, deberá llamar a los acreedores involucrados. La información que no pueda explicarse también debe notificarse a la policía local o a la oficina del alguacil, ya que puede indicar actividad delictiva.

Informe de incidentes. Si detecta transacciones no autorizadas en una cuenta financiera, notifique de inmediato a la compañía de su tarjeta de pago o a su institución financiera. Si detecta cualquier incidente de robo de identidad o fraude, informe inmediatamente el incidente a las fuerzas del orden, a la FTC y al Fiscal General de su estado. Si cree que le han robado su identidad, la FTC le recomienda que tome las siguientes medidas:

- Cierre las cuentas que haya confirmado o que crea que han sido manipuladas o abiertas fraudulentamente. Para ver listas de verificación simplificadas y cartas de muestra que lo guiarán a través del proceso de recuperación, visite https://www.identitytheft.gov/.
- Presentar una denuncia policial local. Obtenga una copia de la denuncia policial y envíela a sus acreedores y a cualquier otra persona que pueda requerir prueba del delito de robo de identidad.

Puede comunicarse con la FTC para obtener más información sobre cómo protegerse de convertirse en víctima de robo de identidad y sobre alertas de fraude y congelación de seguridad:

Centro de Respuesta al Consumidor de la Comisión Federal de Comercio
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (438-4338)
www.ftc.gov/idtheft/

Considere la posibilidad de colocar una Alerta de Fraude en su Expediente de Crédito. Para protegerse contra un posible robo de identidad, considere la posibilidad de colocar una alerta de fraude en su expediente de crédito. Una alerta de fraude le ayuda a protegerse contra la posibilidad de que un ladrón de identidad abra nuevas cuentas de crédito a su nombre. Cuando un comerciante verifica el historial de crédito de alguien que solicita crédito, el comerciante recibe un aviso de que el solicitante puede ser víctima de un robo de identidad. La alerta notifica al comerciante que tome medidas para verificar la identidad del solicitante. Puede colocar una alerta de fraude en su informe de crédito llamando a cualquiera

de los números gratuitos que se proporcionan a continuación. Usted se comunicará con un sistema telefónico automatizado que le permitirá marcar su expediente con una alerta de fraude en las tres agencias de informes de crédito del consumidor. Para obtener más información sobre las alertas de fraude, también puede comunicarse con la FTC como se describió anteriormente.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 2002 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Considere la posibilidad de colocar una congelación de seguridad en su expediente de crédito. Es posible que desee colocar una "congelación de seguridad" (también conocida como "congelación de crédito") en su expediente de crédito. Una congelación de seguridad está diseñada para evitar que los acreedores potenciales accedan a su expediente de crédito en las agencias de informes de crédito del consumidor sin su consentimiento. *A diferencia de una alerta de fraude, usted debe colocar una congelación de seguridad en su expediente de crédito en cada agencia de informes de crédito del consumidor en forma individual*. No se aplica ningún cargo por solicitar, levantar temporalmente o eliminar permanentemente una congelación de seguridad con cualquiera de las agencias de informes de crédito del consumidor. Para obtener más información sobre congelaciones de seguridad, puede comunicarse con las tres agencias nacionales de informes de crédito del consumidor o con la FTC según se describe anteriormente. Dado que las instrucciones para establecer una congelación de seguridad difieren de un estado a otro, comuníquese con las tres agencias nacionales de informes de crédito del consumidor para obtener más información.

Equifax	Congelación de seguridad de Equifax P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Congelación de seguridad de Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

Las agencias de informes de crédito del consumidor pueden requerir una identificación adecuada antes de cumplir con su solicitud. Por ejemplo, es posible que se le pida que proporcione:

- Su nombre completo con la inicial del segundo nombre y la generación (como Jr., Sr., II, III)
- Su número de Seguro Social
- Su fecha de nacimiento
- Direcciones dónde ha vivido en los últimos cinco años
- Una copia legible de una tarjeta de identificación emitida por el gobierno (como una licencia de conducir estatal o una tarjeta de identificación militar)
- Prueba de su dirección residencial actual (como una factura de servicios públicos o un estado de cuenta actual)
- Tarjeta del Seguro Social, recibo de pago o W2
- Si usted es víctima de un robo de identidad, incluya una copia de la denuncia policial, la denuncia de investigación o una queja a una agencia de cumplimiento de la ley en relación con el robo de identidad.

Información adicional para residentes de Massachusetts.

En virtud de la ley de Massachusetts, usted tiene derecho a obtener cualquier denuncia policial presentada con respecto a este incidente. Si usted es víctima de un robo de identidad, también tiene derecho a presentar una denuncia policial y obtener una copia de la misma.

La ley de Massachusetts también permite a los consumidores colocar una congelación de seguridad en sus informes de crédito. Una congelación de seguridad prohíbe que una agencia de informes de crédito divulgue cualquier información del informe de crédito de un consumidor sin autorización por escrito. Sin embargo, tenga en cuenta que colocar una congelación de seguridad en su informe de crédito puede demorar, interferir o impedir la aprobación oportuna de cualquier solicitud que usted realice de nuevos préstamos, hipotecas de crédito, empleo, vivienda u otros servicios. Ya no se aplica un cargo por colocar, levantar o retirar una congelación de seguridad.

Para colocar una congelación de seguridad en su informe de crédito, debe enviar una solicitud por escrito a **cada** una de las tres principales agencias de informes de crédito del consumidor: Equifax (www.equifax.com); Experian (www.experian.com); y TransUnion (www.transunion.com) por correo regular, certificado o urgente a las siguientes direcciones:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348

Experian Security Freeze P.O. Box 9554 Allen, TX 75013

Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016

Para solicitar una congelación de seguridad, deberá proporcionar la siguiente información:

1. Su nombre completo (incluida la inicial del segundo nombre, así como Jr., Sr., II, III, etc.);
2. Número de Seguro Social;
3. Fecha de nacimiento;
4. Si se ha mudado en los últimos cinco (5) años, proporcione las direcciones en las que ha vivido durante los cinco años anteriores;
5. Prueba de dirección actual, como una factura de servicios públicos o una factura telefónica actuales;
6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir estatal o tarjeta de identificación, identificación militar, etc.)

Las agencias de informes de crédito tienen tres (3) días laborables después de recibir su solicitud para colocar una congelación de seguridad en su informe de crédito. Las agencias de información de crédito también deben enviarle una confirmación por escrito en el transcurso de cinco (5) días laborables y proporcionarle un número de identificación personal (PIN) o contraseña únicos, o ambos, que usted pueda utilizar para autorizar la eliminación o el levantamiento de la congelación de seguridad.

Para levantar la congelación de seguridad a fin de permitir el acceso de una entidad específica o una persona física a su informe de crédito, debe llamar o enviar una solicitud por escrito a las agencias de informes de crédito por correo e incluir la identificación adecuada (nombre, dirección, y el número de seguro social) y el número PIN o contraseña que se le proporcionó cuando colocó la congelación de seguridad, así como las identidades de aquellas entidades o personas que desea recibir su informe de crédito o el período de tiempo específico durante el cual desea que esté disponible el informe de crédito. Las agencias de informes de crédito tienen tres (3) días laborables después de recibir su solicitud de levantar la congelación de seguridad para esas entidades identificadas o durante el período de tiempo especificado.

Para eliminar la congelación de seguridad, debe enviar una solicitud por escrito a cada una de las tres agencias de información de crédito por correo e incluir la identificación adecuada (nombre, dirección y número de seguro social) y el número PIN o contraseña que se le proporcionó cuando colocó la congelación de seguridad. Las agencias de información de crédito tienen tres (3) días laborables después de recibir su solicitud para eliminar la congelación de seguridad.

Para residentes de Nueva York. Puede obtener información de la Oficina del Fiscal General del Estado de Nueva York sobre cómo protegerse del robo de identidad y consejos sobre cómo proteger su privacidad en línea. Puede comunicarse con la Oficina del Fiscal General del Estado de Nueva York en:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (llamada gratuita)
1-800-788-9898 (línea gratuita de TDD/TTY)
https://ag.ny.gov

Oficina de Internet y Tecnología (Bureau of Internet and Technology, BIT)
28 Liberty Street
Nueva York, NY 10005
Teléfono: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

Para residentes de Carolina del Norte. Puede obtener información de la Oficina del Fiscal General de Carolina del Norte sobre cómo prevenir el robo de identidad. Puede comunicarse con el Fiscal General de Carolina del Norte en:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (llamada gratuita en Carolina del Norte)
(919) 716-6400
www.ncdoj.gov