Seth Berman
Direct Line: (617) 439-2338
Fax: (617) 310-9338
E-mail: sberman@nutter.com

November 14, 2023

VIA EMAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

My firm represents Shield Packaging Co., Inc. ("Shield"), a company with a principal place of business located at 99 University Road, Canton, Massachusetts 02021. Pursuant to N.H. RSA § 359- C:20, I am writing to notify you of a data breach involving the personal information of 21 New Hampshire residents.

On April 18, 2023, Shield was the victim of an attempted ransomware attack that shut down some of its computers. Shield was able to first shutdown and rebuild its systems without paying a ransom. Immediately upon learning of the attack, Shield engaged a leading digital forensics expert to help them understand what had occurred; determine whether any data had been accessed or taken; and determine what they could do to improve their security. After completing its review, the forensic expert found no evidence that any data had been exfiltrated by the attackers. Nevertheless, Shield instructed the forensic expert to monitor the dark web for any information that might have originated from their servers. On August 24, 2023, the forensic experts notified Shield that the attacker posted on its dark website a small number of confidential documents apparently originating from Shield's computers. These limited documents suggested the possibility that the April attackers may have been able to access other data on some of Shield's computers. Shield then began a detailed review of the potentially impacted computers. Based on this review, Shield found other documents on the relevant computers that contained the PII of approximately 21 New Hampshire residents. Though we do not know if the attackers accessed these records, Shield decided to notify the relevant individuals. At this time, Shield is not aware of any evidence that there has been any attempt to misuse the information of any individual.

As a result of this chain of events, the attackers may have had access to PII including individuals' .

The affected individuals have been notified of the incident by written notice on November 14, 2023. A copy of the written consumer notice letter is attached.

Two years of credit monitoring services have been offered to the affected individuals. Shield has notified the FBI of the incident.

If you should have any question or require any additional information regarding this incident, please feel free to contact me.

Very truly yours,

Seth Berman

SPB2:np
Enclosure
6234845.1

SHIELD PACKAGING CO., INC. *
4145 SW Watson Ave. Suite 400
Beaverton, OR 97005

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 14, 2023

Notice of Data Breach

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

What Happened

On April 18, 2023, Shield Packaging, Co., Inc. ("Shield Packaging") was the victim of an attempted ransomware attack that shut down some of our computers. Immediately upon learning of the attack, we engaged a leading digital forensics expert to help us understand what had occurred; determine whether any data had been accessed or taken; and determine what we could do to improve our security. After completing its review, the forensic expert found no evidence that any data had been exfiltrated by the attackers. Nevertheless, we decided in an abundance of caution to monitor the web for any information that might have originated from our servers. On August 24, 2023, we learned that the attackers posted on their website a small number of confidential documents apparently originating from our computers. These documents did not contain any of your personally identifiable information ("PII") but suggested the possibility that the April attackers may have been able to access other data on some of our computers. We then began a detailed review of the potentially impacted computers. Based on this review, we found other documents on the relevant computers that contained your PII as well as the PII of approximately 600 individuals. At this time, we are not aware of any evidence that there has been any attempt to misuse your information or that of any other individual.

We are truly sorry and hope you will take advantage of the services and options described below, which will help you in the event of a problem resulting from the incident described above or from another cause relating to your information.

What Information Was Involved

The information which may have been accessed included: <<variable data>>.

What We Are Doing

As part of our ongoing efforts to help prevent a similar incident from happening in the future, we engaged a forensics expert to help us recover from the incident and advise on steps we can take to improve our data security and resiliency. We have implemented several key improvements to strengthen our security and resiliency.

In addition, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 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.

*Affiliated entities: Harrison Specialty Co., Inc., Harvard Turf Farms, Inc.

What You Can Do

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 .

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Todd A. Johnston
Shield Packaging Co.

(Enclosure)

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. You may also place a security freeze on your credit reports, free of charge. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses above. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information listed above.

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

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, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including 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. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) 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 make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide 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 between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

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.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

SHIELD PACKAGING CO., INC. *
4145 SW Watson Ave. Suite 400
Beaverton, OR 97005

14 de noviembre de 2023

Aviso de filtración de datos

Estimado/a <<First Name>> <<Last Name>>:

Lo que ocurrió

El 18 de abril de 2023, Shield Packaging, Co., Inc. ("Shield Packaging") fue víctima de un intento de ataque de ransomware que apagó algunas de nuestras computadoras. Inmediatamente después de enterarnos del ataque, contratamos a un experto en análisis forense digital para que nos ayudara a comprender qué había ocurrido; determinar si se había accedido o tomado algún dato; y determinar qué podíamos hacer para mejorar nuestra seguridad. Una vez finalizada su revisión, el experto forense no encontró evidencia de que los atacantes hubieran exfiltrado ningún dato. Sin embargo, decidimos como medida de suma precaución monitorear la web en busca de cualquier información que pudiera haberse originado en nuestros servidores. El 24 de agosto de 2023, nos enteramos de que los atacantes publicaron en su sitio web un pequeño número de documentos confidenciales aparentemente procedentes de nuestras computadoras. Estos documentos no contenían ninguna de su información de identificación personal ("PII"), pero sugerían la posibilidad de que los atacantes de abril hubieran podido acceder a otros datos en algunas de nuestras computadoras. Luego comenzamos una revisión detallada de los equipos potencialmente afectados. Sobre la base de esta revisión, encontramos otros documentos en las computadoras relevantes que contenían su PII, así como la PII de aproximadamente 600 personas. En este momento, no tenemos conocimiento de ninguna evidencia de que haya habido algún intento de hacer un uso indebido de su información o de la de cualquier otra persona.

Lo sentimos mucho y esperamos que aproveche los servicios y opciones que se describen a continuación, que le ayudarán en caso de que surja un problema como resultado del incidente descrito anteriormente o de otra causa relacionada con su información.

Qué información se vio involucrada

La información a la que se pudo haber accedido incluyó: <<variable data>>.

Lo que estamos haciendo

Como parte de nuestros esfuerzos continuos para ayudar a prevenir que ocurra un incidente similar en el futuro, contratamos a un experto forense para que nos ayude a recuperarnos del incidente y nos asesore sobre las medidas que

* Entidades afiliadas: Harrison Specialty Co., Inc., Harvard Turf Farms, Inc.

podemos tomar para mejorar la seguridad y la resiliencia de nuestros datos. Hemos implementado varias mejoras clave para fortalecer nuestra seguridad y resiliencia.

Además, ofrecemos servicios de protección contra el robo de identidad a través de IDX, un experto en servicios de recuperación y filtración de datos. Los servicios de protección de identidad de IDX incluyen: 24 meses de monitoreo de crédito y CyberScan, una póliza de reembolso de seguro de $1,000,000, y la administración total de los servicios de recuperación de robo de identidad. Con esta protección, IDX le ayudará a resolver problemas si su identidad se ve comprometida.

Lo que usted puede hacer

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 la imagen QR y utilizando el código de inscripción proporcionado anteriormente. Los representantes de IDX están disponibles de lunes a viernes de 9 a. m. a 9 p. m., hora del este. Tenga en cuenta que la fecha límite para inscribirse es el 14 de febrero de 2024.

Nuevamente, en este momento, no hay evidencia de que se haya hecho un uso indebido de su información. Sin embargo, le animamos a que aproveche al máximo esta oferta de servicios. Los representantes de IDX tienen pleno conocimiento del incidente y pueden responder las preguntas o inquietudes que pueda tener sobre la protección de su información personal.

Para obtener más información

Encontrará instrucciones detalladas para la inscripción en el documento de Pasos recomendados adjunto. Además, deberá hacer referencia al código de inscripción en la parte superior de esta carta al llamar o inscribirse en línea, por lo que le pedimos que no descarte esta carta.

Llame al o visite https://app.idx.us/account-creation/protect para obtener ayuda o para cualquier otra pregunta que pueda tener.

Atentamente.

Todd A. Johnston
Shield Packaging Co.

(Adjunto)

Pasos recomendados para ayudar a proteger su información

1. **Sitio web e inscripción.** Escanee la imagen QR o vaya a https://app.idx.us/account-creation/protect y siga las instrucciones para la inscripción utilizando su código de inscripción proporcionado en la parte superior de la carta.

2. Active el monitoreo de crédito proporcionado como parte de su membresía en la protección de identidad de IDX. El monitoreo incluido en la membresía debe estar activado para que funcione. Nota: Usted debe establecer el crédito y el acceso a una computadora y a internet para usar este servicios. Si necesita ayuda, IDX podrá ayudarlo.

3. Teléfono. Comuníquese con IDX al 1-800-939-4170 para obtener más información sobre este evento y hable con representantes expertos sobre los pasos apropiados que debe tomar para proteger su identidad crediticia.

4. Revise sus informes de crédito. Le recomendamos que se mantenga alerta revisando los extractos de sus cuentas y monitoreando sus informes de crédito. Según la ley federal, también tiene derecho a recibir cada 12 meses una copia gratuita de su informe de crédito de cada una de las tres principales compañías de informes de crédito. Para obtener un informe de crédito anual gratuito, ingrese en www.annualcreditreport.com o llame al 1-877-322-8228. Es posible que desee espaciar sus solicitudes para recibir un informe gratuito de una de las tres agencias de informes de crédito cada cuatro meses.

Si descubre algún elemento sospechoso y se ha inscrito en la protección de identidad IDX, notifíquelo de inmediato llamando o ingresando en el sitio web de IDX y presentando una solicitud de ayuda.

Si presenta una solicitud de ayuda o informa una actividad sospechosa, un miembro de nuestro equipo de Cuidado de identidad de IDX se comunicará con usted y le ayudará a determinar la causa de la información sospechosa. En el improbable caso de que sea víctima de un robo de identidad como consecuencia de este incidente, se le asignará un especialista en atención a la identidad que trabajará en su nombre para identificar, detener y revertir el daño rápidamente.

También debe saber que tiene derecho a presentar una denuncia policial si alguna vez sufre un fraude de identidad. Tenga en cuenta que para presentar una denuncia de delito o incidente ante las autoridades policiales por robo de identidad es probable que tenga que aportar algún tipo de prueba de que ha sido víctima de ello. Con frecuencia se requiere una denuncia policial para impugnar información fraudulenta. Puede reportar incidentes sospechosos de robo de identidad a la policía local o al Fiscal General.

5. Coloque alertas de fraude en las tres agencias de crédito. Si elige colocar una alerta de fraude, le recomendamos que lo haga después de activar su monitoreo de crédito. Puede colocar una alerta de fraude en una de las tres principales agencias de crédito por teléfono y también a través del sitio web de Experian o Equifax. Una alerta de fraude le dice a los acreedores que sigan ciertos procedimientos, incluso que se comuniquen con usted, antes de que abran cuentas nuevas o cambien sus cuentas existentes. Por esa razón, la colocación de una alerta de fraude puede protegerlo, pero también puede hacer que se retrase la obtención de crédito. La información de contacto de las tres agencias es la siguiente:

Agencias de informes de crédito

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

Es necesario comunicarse con solo con UNA de estas agencias y utilizar solo UNO de estos métodos. Tan pronto como una de las tres agencias confirme su alerta de fraude, se notifica a las demás que también coloquen alertas en sus registros.

Recibirá cartas de confirmación por correo y luego podrá solicitar los tres informes de crédito, de forma gratuita, para su revisión. Una alerta de fraude inicial durará un año.

Tenga en cuenta: nadie puede colocar una alerta de fraude en su informe de crédito, excepto usted.

6. Congelamiento de seguridad. También puede colocar un congelamiento de seguridad en sus informes de crédito de forma gratuita. Un congelamiento 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 establecer un congelamiento de seguridad en su informe de crédito puede demorar, interferir o impedir la aprobación oportuna de cualquier solicitud que presente para nuevos préstamos, créditos, hipotecas, empleo, vivienda u otros servicios. Según la ley federal, no se le puede cobrar por colocar, levantar o eliminar un congelamiento de seguridad. Debe presentar su solicitud de congelamiento ante cada una de las tres principales agencias de informes del consumidor: Equifax (www.equifax.com), Experian (www.experian.com) y TransUnion (www.transunion.com). Para colocar un congelamiento de seguridad en su informe de crédito, puede enviar una solicitud por escrito por correo ordinario, certificado o de entrega de un día para otro a las siguientes direcciones. También puede colocar un congelamiento de seguridad en cada uno de los sitios web de las agencias de informes del consumidor o por teléfono, utilizando la información de contacto arriba detallada.

Para solicitar un congelamiento de seguridad, deberá proporcionar parte o la totalidad de la siguiente información a la agencia de informes de crédito, dependiendo de si lo hace en línea, por teléfono o por correo postal:

1. 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, las direcciones donde ha vivido durante los últimos cinco años;
5. Prueba de la dirección actual, tal como una factura de servicios públicos actual, factura telefónica, contrato de alquiler o escritura;
6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir o tarjeta de identificación estatal, identificación militar, etc.);
7. Tarjeta de Seguro Social, talón de pago o W2;
8. Si usted es víctima de robo de identidad, incluya una copia de la denuncia policial, el informe de la investigación o la reclamación ante agencia de orden público en relación con el robo de identidad.

Las agencias de informes de crédito tienen de uno (1) a tres (3) días hábiles después de recibir su solicitud para colocar un congelamiento de seguridad en su informe de crédito, según el método de su solicitud. Las agencias de crédito también deben enviarle una confirmación por escrito dentro de los cinco (5) días hábiles y proporcionarle un número de identificación personal (PIN) o contraseña (o ambos) exclusivos que usted puede usar para autorizar la eliminación o el levantamiento del congelamiento de seguridad. Es importante mantener este PIN/contraseña en un lugar seguro, ya que lo necesitará para levantar o eliminar el congelamiento de seguridad.

Para levantar el congelamiento de seguridad con el fin de permitir que una entidad o individuo específico acceda a su informe de crédito, debe hacer una solicitud a cada una de las agencias de informes de crédito por correo postal, a través de su sitio web o por teléfono (utilizando la información de contacto anterior). Debe proporcionar una identificación adecuada (incluido el nombre, la dirección y el número de seguro social) y el número PIN o la contraseña que se le proporcionó cuando colocó el congelamiento de seguridad, así como las identidades de las entidades o personas a las que le gustaría recibir su informe de crédito. También puede levantar temporalmente un congelamiento de seguridad durante un período de tiempo específico en lugar de hacerlo para una entidad o persona específica, utilizando la misma información de contacto arriba proporcionada. Las agencias de crédito tienen entre una (1) hora (para solicitudes realizadas en línea) y tres (3) días hábiles (para solicitudes realizadas por correo postal) después de recibir su solicitud para levantar el congelamiento de seguridad para esas entidades identificadas o durante el período de tiempo especificado.

Para eliminar el congelamiento de seguridad, debe realizar una solicitud a cada una de las agencias de informes de crédito por correo postal, a través de su sitio web o por teléfono (utilizando la información de contacto arriba proporcionada). Debe proporcionar una identificación adecuada (nombre, dirección y número de seguro social) y el número PIN o

contraseña que se le proporcionó cuando colocó el congelamiento de seguridad. Las agencias de crédito tienen entre una (1) hora (para solicitudes realizadas en línea) y tres (3) días hábiles (para solicitudes realizadas por correo postal) después de recibir su solicitud para eliminar el congelamiento de seguridad.

7. Puede obtener más información de las siguientes agencias sobre las medidas que puede tomar para prevenir el robo de identidad. La Comisión Federal de Comercio también anima a quienes descubran que se ha hecho un uso indebido de la información a que presenten una reclamación ante ellos.

Residentes de California: Visite la Oficina de Protección de Privacidad de California (www.oag.ca.gov/privacy) para más información sobre protección contra el robo de identidad. Oficina del Fiscal General de California, 1300 I Street, Sacramento, CA 95814, Teléfono: 1-800-952-5225.

Residentes de Kentucky: Oficina del Fiscal General de Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Teléfono: 1-502-696-5300.

Residente de Maryland: Oficina del Fiscal General de Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Teléfono: 1-888-743-0023.

Residentes de Massachusetts: Conforme a la ley de Massachusetts, usted tiene derecho a obtener cualquier informe policial presentado con respecto a este incidente. Si es víctima de un robo de identidad, también tiene derecho a presentar una denuncia policial y obtener una copia de ella.

Residentes de Nuevo México Tiene derechos de acuerdo con la Ley de Informes de Crédito Justos, como el derecho a ser informado si los datos de su expediente de crédito han sido utilizados en su perjuicio, el derecho a saber lo que figura en su expediente de crédito, el derecho a solicitar su calificación crediticia y el derecho a objetar información incompleta o inexacta. Además, de conformidad con la Ley de Informes de Crédito Justos, las agencias de informes crediticios deben corregir o eliminar información inexacta, incompleta o no verificable; las agencias de informes crediticios no pueden informar información negativa obsoleta; el acceso a su expediente es limitado; debe dar su consentimiento para que se proporcionen informes crediticios a los empleadores; puede limitar las ofertas de crédito y seguro "preseleccionadas" que obtiene en función de la información en su informe de crédito; y puede solicitar daños y perjuicios a los infractores. Usted puede tener derechos adicionales conforme a la Ley de Informes de Crédito Justos, que no figuran aquí. Las víctimas del robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos conforme a la Ley de Informes de Crédito Justos. Le animamos a que consulte sus derechos conforme a la Ley de Informes de Crédito Justos visitando www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o escribiendo al Centro de respuesta al consumidor a: Consumer Response Center, Room 130-A, Comisión Federal de Comercio, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Residentes de Nueva York: el Fiscal General puede ser contactado en: Oficina del Fiscal General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

Residentes de Carolina del Norte: Oficina del Fiscal General de Carolina del Norte**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Teléfono: 1-919-716-6400.

Residentes de Oregon: Departamento de Justicia de Oregon, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Teléfono: 877-877-9392

Residentes de Rhode Island Oficina del Fiscal General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Teléfono: 401-274-4400

Todos los residentes estadounidenses: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.