



Lauren D. Godfrey
One PPG Place, 28th Floor
Pittsburgh, Pennsylvania 15222
Lauren.Godfrey@lewisbrisbois.com
Direct: 412.567.5113

November 1, 2022

File No. 52570.02

VIA EMAIL TO: ldtheft@oag.state.md.us

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Morrison Products ("Morrison") with locations in Texas and Mexico in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute, Md. Code Ann. Comm. Law §§ 14-3501 - 3508.

1. Nature of the Security Incident

On February 25, 2022, Morrison discovered it was the victim of a ransomware attack. In response, Morrison immediately took steps to terminate the activity and to secure its network, systems, and data. In addition, Morrison retained an independent forensic investigation company and incident response professionals to conduct a forensic investigation into the incident, assist with recovery and remediation efforts and with determining what happened. Due to the widespread encryption, recovery efforts took through June 6, 2022 to complete.

The forensic investigation determined that the attackers had access to files stored within Morrison's systems. Although Morrison worked diligently to identify which of its employees' information may have been involved in the incident, Morrison was unable to determine exactly whose information was impacted. Accordingly, out of an abundance of caution, Morrison determined to notify all potentially impacted current and former employees of the incident. Following Morrison's internal review of its records, Morrison worked to identify current address information which was ultimately completed on October 18, 2022, following a National Change of Address search and completion of English and Spanish versions of its consumer letter so all potentially impacted individuals could be notified concurrently about the incident.

On November 1, 2022, Morrison will be notifying all potentially impacted individuals of the incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for approximately 2 Maryland residents. The information involved in the incident may differ depending on the individual but may include the following for affected Maryland residents: name, address, and social security number.

3. Notification to Affected Individuals

On November 1, 2022, notification letters will be sent to affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to, including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

In response to the incident, Morrison retained cybersecurity experts and launched a forensics investigation to assist with recovery and remediation efforts, determine the source and scope of the compromise, and to further secure its network. Morrison is in the process of implementing additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

In addition, Morrison has reported the incident to the Federal Bureau of Investigation ("FBI") and will cooperate fully to assist with any investigation.

Finally, Morrison is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above and reporting the incident to nationwide consumer reporting agencies (i.e., Equifax, Experian, and Transunion).

5. **Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at Lauren.Godfrey@lewisbrisbois.com or 412.567.5113.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LDG:mff

Encl.: Sample Notification Letter

cc: Michael F. Ferragamo, Lewis Brisbois (Michael.Ferragamo@lewisbrisbois.com)



P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-909-4421
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

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

November 1, 2022

Notice of Data <<Variable Data 2>>

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

Morrison Products takes the privacy and security of your information very seriously. Thus, we are informing you of a data security incident that may have involved your personal information. This notice explains the incident, provides you with steps you can take to protect your information, and offers you complimentary credit monitoring and identity protection services.

What happened? On February 25, 2022, our IT team detected unusual activity in our systems. In response, we immediately shut down some systems and began an investigation with the help of third-party cybersecurity experts and incident response professionals. After a thorough investigation, it was determined that on or about February 10, 2022, an outside party gained access to our computer systems, including potentially those that store information relating to your employment with us. Because we take this incident seriously, Morrison diligently worked to assess what information of yours was stored on our systems. However, despite this thorough review, the investigation team was unable to determine whether your specific information was accessed or taken. Out of an abundance of caution, we are notifying you to provide you with steps you can take to protect your information.

What Information Was Involved? The information that was stored in our system varied but potentially could have included things such as your name, <<Variable Data 3>>.

What We Are Doing: In addition to the steps described above, we are working with cybersecurity experts to enhance the security of our digital environment and prevent a similar incident from occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrators accountable. Additionally, we are offering you complimentary identity theft protection services through IDX. These services include: [12 months/24 months] of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

What You Can Do: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-909-4421 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the enrollment deadline is February 1, 2023. Again, at this time, there is no evidence that your information has been misused.

For More Information: Please call 1-833-909-4421 or go to <https://app.idx.us/account-creation/protect> for help or for any questions you may have. 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.

Sincerely,

Anne Holmes Schuerger
Morrison Products, Inc.
(Enclosure)



P.O Box 989728
West Sacramento, CA 95798-9728

Para inscribirse, por favor llame al:
1-833-909-4421
o visite:
<https://app.idx.us/account-creation/protect>
Código de inscripción:
<<Enrollment Code>>

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

1 de noviembre de 2022

Comunicado sobre los datos <<Variable Data 2>>

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

Morrison Products se toma muy en serio la privacidad y la seguridad de su información. Por esta razón, le notificamos un incidente en la seguridad de los datos que puede haber comprometido su información personal. Este comunicado explica el incidente, le brinda las medidas que puede tomar para proteger su información y le ofrece servicios gratuitos de monitoreo de crédito y protección de identidad.

¿Qué sucedió? El 25 de febrero de 2022, nuestro equipo de expertos en informática (TI) detectó actividad inusual en nuestros sistemas. En consecuencia, desactivamos inmediatamente algunos sistemas e iniciamos una investigación con la ayuda de terceros expertos en ciberseguridad y profesionales especializados en la resolución de incidentes. Después de una investigación exhaustiva, se determinó que el 10 de febrero de 2022, o alrededor de ese día, un tercero tuvo acceso a nuestros sistemas informáticos, incluso potencialmente a los que almacenan información relacionada a su empleo con nosotros. Dado que nos tomamos muy en serio este incidente, Morrison ha trabajado con diligencia para evaluar qué información de usted se almacenaba en nuestros sistemas. Sin embargo, a pesar de esta revisión exhaustiva, el equipo de investigación no pudo determinar si se accedió o se sustrajo información específica sobre usted. Como medida de seguridad, le ofrecemos medidas que puede tomar para proteger su información.

¿Qué información estuvo en juego? La información que se almacenaba en nuestro sistema era diversa, pero pudo haber incluido datos como su nombre, <<Variable Data 3>>.

Qué estamos haciendo: Además de las medidas descritas anteriormente, estamos trabajando con expertos en ciberseguridad para incrementar la seguridad de nuestro entorno digital y evitar que se produzca un incidente similar en el futuro. También hemos dado aviso a la Oficina Federal de Investigación (FBI) y ofreceremos toda la ayuda necesaria para que los responsables respondan por sus actos. Además, le ofrecemos servicios complementarios de protección contra el robo de identidad a través de IDX. Estos servicios incluyen: **[12 months/24 months]** de crédito y monitoreo CyberScan, una póliza de seguro de reembolso de \$1,000,000 de dólares y servicios de recuperación de robos de identidad totalmente supervisados.

Lo que usted puede hacer: Le invitamos a ponerse en contacto con IDX si tiene alguna duda y a inscribirse en los servicios gratuitos de protección de la identidad llamando al 1-833-909-4421 o visitando <https://app.idx.us/account-creation/protect> utilizando el código de inscripción indicado anteriormente. Los representantes de IDX están disponibles de lunes a viernes de 9 am a 9 pm en el horario del Este. Tenga en cuenta que el plazo para inscribirse es 1 de febrero de 2023. Reiteramos que, en este momento, no hay evidencia de que se haya hecho uso indebido de su información.

Para mayor información: Favor de llamar al 1-833-909-4421 o visitar <https://app.idx.us/account-creation/protect> para recibir ayuda o aclarar dudas. Además, tendrá que hacer referencia al código de inscripción que aparece en la parte superior de esta carta cuando llame o se inscriba en línea, así que no tire esta carta.

Atentamente,

Anne Holmes Schuerger
Morrison Products, Inc.
(Anexo)

16900 S. Waterloo Road | Cleveland, Ohio 44110

Medidas recomendadas para ayudar a proteger su información

1. Página web e inscripción. Vaya a <https://app.idx.us/account-creation/protect> y siga las instrucciones para la inscripción utilizando el código de inscripción que se le indica en la parte superior de la carta.

2. Active el monitoreo de crédito ofrecido como parte de su membresía de protección de identidad de IDX. El monitoreo incluido en la membresía deberá ser activado para que sea efectivo. Nota: Para utilizar este servicio, deberá tener un crédito adquirido y acceso a una computadora e Internet. Si necesita ayuda, IDX podrá atenderle.

3. Teléfono. Contacte a IDX al 1-833-909-4421 para obtener información adicional sobre este evento y hablar con representantes expertos sobre las medidas adecuadas para proteger su identidad crediticia.

4. Revise sus informes crediticios. Le recomendamos que permanezca atento revisando los estados de cuenta y monitoreando los informes crediticios. Según la ley federal, también tiene derecho a recibir cada 12 meses una copia gratuita de su informe crediticio de cada una de las tres principales agencias de información crediticia. Para obtener sin costo un informe crediticio anual, vaya a www.annualcreditreport.com o llame al 1-877-322-8228. Es posible que desee escalonar sus solicitudes para recibir un informe gratuito cada cuatro meses por parte de una de las tres agencias de crédito. Si detecta algún hecho sospechoso y se ha inscrito en la protección de identidad IDX, notifíquelo inmediatamente llamando o entrando en el sitio web de IDX y presente una solicitud de ayuda. Si presenta una solicitud de ayuda o denuncia una actividad sospechosa, le contactará un agente de nuestro equipo ID Care que le ayudará a determinar la causa de los hechos sospechosos. En el improbable caso de que sea víctima de un robo de identidad como consecuencia de este incidente, se le asignará un especialista de ID Care que actuará 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 es víctima de un fraude de identidad. Tenga en cuenta que, para presentar una denuncia de delito o un informe de incidente ante la policía por robo de identidad, probablemente deba ofrecer algún tipo de prueba para acreditarlo. A menudo se requiere un informe policial para reclamar asuntos de carácter fraudulento. Puede denunciar los incidentes sospechosos de robo de identidad a las autoridades locales o al Fiscal General.

5. Envíe alertas de fraude a las tres agencias de crédito. Si decide colocar una alerta de fraude, le recomendamos que lo haga después de activar su monitoreo de crédito. Puede enviar una alerta de fraude a una de las tres principales agencias de crédito, ya sea por teléfono o a través del sitio web de Experian o Equifax. Una alerta de fraude avisa a los acreedores de que deberán seguir ciertos procedimientos, entre ellos ponerse en contacto con usted, antes de abrir nuevas cuentas o modificar las que ya tiene. Por ello, enviar una alerta de fraude puede protegerle, pero también puede retrasarle a la hora de obtener un crédito. Los datos de contacto de las tres oficinas son los siguientes:

Agencias de crédito

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

Es necesario ponerse en contacto con sólo UNA de estas oficinas y utilizar sólo UNO de estos medios. En cuanto una de las tres agencias confirme su alerta de fraude, se notifica a las demás para que también emitan alertas en sus registros. Usted recibirá cartas de confirmación por correo postal y entonces podrá solicitar los tres informes crediticios, sin costo alguno, para su revisión. Una alerta de fraude inicial durará un año.

Por favor tome en cuenta que: Nadie puede enviar una alerta de fraude sobre su informe crediticio, excepto usted.

6. Congelamiento de cuentas. Al establecer un congelamiento de cuentas, la persona que de manera fraudulenta adquiera información de identificación personal de usted, no podrá utilizar dicha información para abrir nuevas cuentas o pedir un

préstamo a su nombre. Deberá ponerse en contacto con las tres oficinas nacionales de información crediticia indicadas anteriormente para aplicar el bloqueo. Tenga en cuenta que, cuando usted aplique el congelamiento de cuentas, no podrá pedir dinero prestado, obtener crédito inmediato, o una nueva tarjeta de crédito, hasta que retire de forma temporal o permanente el bloqueo. Congelar o descongelar sus expedientes crediticios no tiene ningún costo.

7. Puede obtener información adicional sobre las acciones que puede emprender para evitar el robo de identidad en las siguientes agencias. La Comisión Federal de Comercio también invita a quienes detecten que su información ha sido utilizada de forma indebida, a presentar una reclamación con ellos.

Residentes de California: Visite la Oficina de Protección de la Privacidad de California (www.oag.ca.gov/privacy) para información adicional sobre la 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.

Residentes de Maryland: Oficina del Fiscal General de Maryland, División de Protección al Consumidor 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Teléfono: 1-888-743-0023.

Residentes de Nuevo México: Usted tiene derechos, de acuerdo con la Ley de Información Crediticia Equitativa (FCRA), tales como el derecho a que se le notifique si la información de su expediente de crédito ha sido utilizada en su contra, el derecho a saber lo que hay en su expediente de crédito, el derecho a preguntar por su puntuación de crédito y el derecho a impugnar la información incompleta o inexacta. Además, de acuerdo con la Ley de Información Crediticia Equitativa, las agencias de informes de los consumidores deberán corregir o suprimir la información inexacta, incompleta o no verificable; las agencias de informes de los consumidores no podrán comunicar información negativa obsoleta; el acceso a su expediente está limitado; usted debe dar su consentimiento para que los informes crediticios se proporcionen a los empleadores; puede limitar las ofertas de crédito y de seguro "preseleccionadas" que reciba basándose en la información contenida en su informe crediticio; y puede solicitar una indemnización por daños y perjuicios al infractor. Es posible que tenga otros derechos en virtud de la Ley de Información Crediticia Equitativa que no se han resumido aquí. Las víctimas del robo de identidad y el personal militar en activo tienen derechos adicionales específicos en virtud de la Ley de Información Crediticia Equitativa. Puede consultar sus derechos en virtud de la Ley de Información Crediticia Equitativa visitando www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o escribiendo al Centro de Respuesta al Consumidor, Sala 130-A, Comisión Federal de Comercio, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Residentes en Nueva York: se puede contactar al Fiscal General en: Oficina del Fiscal General, El Capitolio, 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 Centro de Servicio Postal 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: 1-877-877-9392.

Residentes de Rhode Island: Oficina de Fiscal General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Teléfono: 1-401-274-4400.

Todos los residentes en EE.UU: Centro de Información sobre el Robo de Identidad, Comisión Federal de Comercio, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Recommended Steps to help Protect your Information

1. 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.

2. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. 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.

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: 1-877-877-9392.

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

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.