



Orrick, Herrington & Sutcliffe LLP

401 Union St
Suite 3300
Seattle, WA 98101

+1 206-839-4300

orrick.com

Joseph Santiesteban

E JSantiesteban@orrick.com

D +1 206-839-4300

F +1 206-839-4301

September 25, 2023

By E-Mail

Attorney General of Maryland

Idtheft@oag.state.md.us

RE: Notice of Security Event Relating to Maryland Residents / U.S. Waffle, Inc.

Dear Attorney General:

We are writing on behalf of our client, U.S. Waffle, Inc (“U.S. Waffle” or the “Company”), to notify you of a security event. U.S. Waffle was alerted to an employee email account was accessed by an unauthorized actor. U.S. Waffle promptly took steps to stop the activity and launched an internal investigation with the support of a forensics IT expert. U.S. Waffle also notified law enforcement. U.S. Waffle recently determined that personal information was in the affected email accounts and may have been downloaded between January 18, 2023 and March 3, 2023.

Affected information may include the data provided for maintaining human resources files, including date of birth, Social Security Number, Align Registration ID, passport number, driver’s license number, tax ID, birth and/or marriage certificate, account number, routing number, credit card number, security code and/or PIN number, medical information, or health insurance information. On June 30, 2023, U.S. Waffle identified the personal information relating to residents of Maryland. The purpose of the access appears to have been to defraud U.S. Waffle and redirect supplier payments to an unauthorized account. U.S. Waffle does not have reason to believe the actor targeted the personal information specifically. U.S. Waffle is not aware of any misuse of the personal information.

U.S. Waffle is committed to safeguarding its systems and information. As part of its ongoing commitment to privacy of U.S. Waffle personal information, U.S. Waffle has taken steps to deploy additional safeguards onto our systems, including reinforcing our security, authentication, and verification practices, reviewing our systems to enhance security monitoring and controls.

The information of approximately one (1) Maryland resident was affected in the incident. The Company notified the Maryland resident via U.S. postal mail on September 25, 2023. A sample notice is attached as Attachment A.

If your office requires any further information in this matter, please contact me at +1 206-839-4300 or JSantiesteban@orrick.com.

Sincerely,

/s/Joseph Santiesteban

Partner

Orrick, Herrington, & Sutcliffe, LLP



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

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

Re: Notice of Security Event

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

U.S. Waffle, Inc ("U.S. Waffle") recently experienced a security event. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring and identity restoration services.

What happened?

An employee email account was accessed by an unauthorized actor. We promptly took steps to stop the activity and launched an investigation with the support of a forensics expert. We also coordinated with law enforcement.

What information was involved?

We recently determined that, your personal information was in the affected email accounts and may have been downloaded between January 18, 2023 and March 3, 2023. The affected information includes: <<b2b_text_1 (Data Elements)>><<b2b_text_2 (Data Elements cont.)>>.

The purpose of the access appears to have been to redirect payments, and we don't have reason to believe the actor targeted your information specifically. We also are not aware of any misuse of your information.

What we are doing:

We are offering two years of complimentary identity monitoring services through Kroll. Please see Attachment A for details regarding these complimentary identity monitoring services, as well as how to activate with your unique code. **You must enroll by <<b2b_text_6 (activation deadline)>> to receive these services.**

U.S. Waffle is committed to safeguarding confidential and sensitive information and has taken additional steps to deploy additional safeguards onto our systems, including reinforcing our security, authentication, and verification practices, reviewing our systems to enhance security monitoring and controls.

What you can do:

In addition to activating the identity monitoring services being offered to you at no charge, we encourage you to take the following precautions:

- It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to help protect your identity is contained in Attachment B.

For more information:

U.S. Waffle has established a dedicated call center to answer questions about the security event as well as the Kroll services that we are offering to you. If you have any questions, please call the call center at (866) 731-2895 Monday through Friday from 9:00 a.m. to 6:30 p.m. ET, excluding some major U.S. holidays.

Sincerely,

John Symons
Chief Executive Officer
U.S. Waffle, Inc.

Attachment A – Kroll Instructions

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Attachment B – Information for U.S. Residents

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll free +1 (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might help protect against someone else obtaining credit in your name.

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. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax

Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
(888) 766-0008
www.equifax.com

Experian

Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

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

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, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to help protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (877) 566-7226 (Toll-free within North Carolina); +1 (919) 716-6400; or www.ncdoj.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; +1 (800) 771-7755; or www.ag.ny.gov.

For California, New York, North Carolina, and Washington residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s)



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

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

Re: Aviso de evento de seguridad

Estimado <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

US Waffle, Inc ("US Waffle") experimentó recientemente un evento de seguridad. Lea atentamente este aviso, ya que proporciona información actualizada sobre lo que sucedió y lo que estamos haciendo, así como información sobre cómo puede obtener servicios gratuitos de monitoreo de crédito y restauración de identidad.

¿Qué sucedió?

Un actor no autorizado accedió a la cuenta de correo electrónico de un empleado. Rápidamente tomamos medidas para detener la actividad e iniciamos una investigación con el apoyo de un experto forense. También coordinamos con las autoridades.

¿Qué información se vio involucrada?

Recientemente determinamos que su información personal estaba en las cuentas de correo electrónico afectadas y pudo haberse descargado entre el 18 de enero de 2023 y el 3 de marzo de 2023. La información afectada incluye: <<b2b_text_3 (Data ElementsESP)>><<b2b_text_4 (Data ElementsESP cont.)>>.

El propósito del acceso parece haber sido redirigir los pagos y no tenemos motivos para creer que el actor se haya dirigido a su información de forma específica. Tampoco hemos tenido conocimiento de algún uso incorrecto de su información.

Lo que estamos haciendo:

Le ofrecemos dos años de servicios de monitoreo de identidad gratuitos a través de Kroll. Consulte el Anexo A para obtener detalles sobre estos servicios de monitoreo de identidad gratuitos, así como de qué forma activarlos con su código único. **Debe inscribirse para el <<b2b_text_5 (activation deadline)>>** para recibir estos servicios.

US Waffle se compromete a salvaguardar la información confidencial y sensible, y ha tomado medidas adicionales para implementar salvaguardas complementarias en nuestros sistemas, incluido el refuerzo de nuestras prácticas de seguridad, autenticación y verificación, y la revisión de nuestros sistemas para mejorar el monitoreo y los controles de seguridad.

Lo que puede hacer:

Además de activar los servicios de monitoreo de identidad que se le ofrecen sin costo alguno, le recomendamos que tome las siguientes precauciones:

- Siempre es una buena idea permanecer atento a las amenazas de robo de identidad o fraude, además de revisar y monitorear periódicamente sus estados de cuenta e historial crediticio para detectar cualquier señal de transacciones o actividades no autorizadas.
- Si alguna vez sospecha que es víctima de robo de identidad o fraude, puede comunicarse con la policía local. En el adjunto B encontrará información adicional acerca de cómo ayudar a proteger su identidad.

Para obtener más información:

US Waffle ha establecido un centro de llamadas exclusivo para responder preguntas sobre el evento de seguridad, así como los servicios de Kroll que le ofrecemos. Si tiene alguna pregunta, comuníquese con el centro de llamadas al (866) 731-2895 de lunes a viernes, de 9:00 a. m. a 6:30 p. m. (ET, hora del este), excluyendo algunos días festivos importantes de EE. UU.

Atentamente,

John Symons
Director ejecutivo
U.S. Waffle, Inc.

Anexo A: Instrucciones de Kroll

Visite <https://enroll.krollmonitoring.com> para activar los servicios de monitoreo de identidad y aprovecharlos.

Tiene hasta el <<b2b_text_5 (activation date)>> para activar sus servicios de monitoreo de identidad.

Número de membresía: <<Membership Number s_n>>

Para obtener más información sobre Kroll y sus servicios de monitoreo de identidad, puede visitar info.krollmonitoring.com.



APROVECHE LOS SERVICIOS DE MONITOREO DE IDENTIDAD

Se le ha brindado acceso a los siguientes servicios de Kroll:

Monitoreo de crédito de una oficina de crédito

Recibirá alertas cuando haya cambios en su información crediticia, por ejemplo, cuando se solicite una nueva línea de crédito a su nombre. Si no reconoce la actividad, tendrá la opción de llamar a un especialista en fraudes de Kroll, que podrá ayudarlo a determinar si se trata de un indicador de robo de identidad.

Asesoría sobre fraudes

Tiene acceso ilimitado para realizar consultas con un especialista en fraudes de Kroll. El asesoramiento incluye mostrarle las formas más efectivas de proteger su identidad, explicarle sus derechos y protecciones en virtud de la ley, ofrecer asistencia con las alertas de fraude e interpretar cómo se accede y utiliza la información personal, incluyendo la investigación de actividades sospechosas que podrían estar vinculadas con un incidente de robo de identidad.

Restauración por robo de identidad

Si resulta ser víctima de un robo de identidad, un investigador experto autorizado de Kroll trabajará en su representación para resolver cualquier problema relacionado. Usted tendrá acceso a un investigador especializado que entiende sus problemas y que puede realizar la mayor parte del trabajo por usted. El investigador podrá investigar a fondo para revelar todos los aspectos del robo de identidad y, luego, trabajar para resolverlo.

El sitio web de activación de Kroll solo es compatible con la versión actual o una versión anterior de Chrome, Firefox, Safari y Edge. Para recibir servicios de crédito, usted debe ser mayor de 18 años y tener un crédito en EE. UU., tener un número de seguro social a su nombre, así como un domicilio de residencia en EE. UU. asociado a su expediente de crédito.

Adjunto B: Información para residentes de los EE. UU.

MÁS INFORMACIÓN SOBRE LA PROTECCIÓN DE IDENTIDAD

INFORMACIÓN PARA OBTENER UN INFORME DE CRÉDITO GRATUITO

Los residentes de EE. UU. tienen derecho, según la ley de EE. UU., a un informe crediticio anual gratuito de cada una de las tres principales agencias de informes crediticios. Para solicitar su informe crediticio gratuito, visite www.annualcreditreport.com o llame sin costo al +1 (877) 322-8228.

INFORMACIÓN SOBRE LA IMPLEMENTACIÓN DE UNA ALERTA DE FRAUDE O CONGELAMIENTO DE SEGURIDAD

Puede comunicarse con las tres principales agencias de crédito en las direcciones que aparecen a continuación para colocar una alerta de fraude en su informe crediticio. Una alerta de fraude notifica a cualquiera que solicite su expediente crediticio que usted sospecha ser víctima de fraude. Una alerta de fraude no afecta su capacidad para obtener un préstamo o crédito. En cambio, alerta a las empresas de que su información personal podría haber estado comprometida y requiere que la empresa verifique su identidad antes de emitir su crédito. Si bien esto puede causar una breve demora si es usted quien solicita el crédito, podría protegerlo en contra de otra persona que busque obtener crédito en su nombre.

Un congelamiento de seguridad prohíbe que una agencia de informes crediticios divulgue cualquier información del informe crediticio de un consumidor sin la debida autorización por escrito. Sin embargo, tenga en cuenta que colocar un congelamiento de seguridad en su informe crediticio puede retrasar, interferir con, o impedir la aprobación oportuna de cualquier solicitud que realice de nuevos préstamos, crédito, hipotecas, empleo, vivienda u otros servicios. Las agencias de informes crediticios no pueden cobrarle por colocar, suspender temporalmente o eliminar permanentemente una congelación de seguridad.

Para colocar una alerta de fraude o congelación de seguridad en su informe de crédito, debe comunicarse con las tres agencias de crédito siguientes:

Equifax

División de Fraude al Consumidor
P.O. Box 740256
Atlanta, GA 30374
(888) 766-0008
www.equifax.com

Experian

Centro de Fraudes Crediticios
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

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

Para solicitar un congelamiento de seguridad, deberá proporcionar la siguiente información:

1. Su nombre completo (inclusive la inicial de su segundo nombre, así como Jr., Sr., II, III, etc.);
2. Número de Seguro Social;
3. Fecha de nacimiento;
4. Si se mudó en los últimos cinco (5) años, incluya los domicilios en los que vivió durante esos últimos cinco años;
5. Comprobante de domicilio actual, por ejemplo, factura actual de servicios públicos o factura telefónica, y
6. Una fotocopia legible de un documento de identidad emitido por el gobierno (licencia de conducir estatal o documento de identidad, identificación militar, etc.).

También puede comunicarse con la Comisión Federal de Comercio de EE. UU. (FTC, Federal Trade Commission) para obtener más información sobre alertas de fraude, congelamientos de seguridad y cómo protegerse contra el robo de identidad. Se puede comunicar con la FTC en 400 7th St. SW, Washington, DC 20024; teléfono +1 (877) 382-4357; o visite www.consumer.gov/idtheft.

RECURSOS ADICIONALES

El fiscal general de su estado también puede brindarle consejos sobre cómo prevenir el robo de identidad, y usted debe denunciar los casos de robo de identidad conocido o sospechado a las autoridades policiales, al fiscal general de su estado o a la FTC.

Residentes de Maryland: Se pueden comunicar con el Procurador General en Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; o www.marylandattorneygeneral.gov.

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

Residentes de Carolina del Norte: Pueden comunicarse con el Fiscal General en 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (877) 566-7226 (llamada gratuita dentro de Carolina del Norte); +1 (919) 716-6400; o www.ncdoj.gov.

Para los residentes de Nueva York: Pueden comunicarse con el Fiscal General a través de la Fiscalía General, The Capitol, Albany, NY 12224-0341; +1 (800) 771-7755; o en www.ag.ny.gov.

Para residentes de California, Nueva York, Carolina del Norte y Washington: pueden obtener una o más (según el estado) copias adicionales de su informe crediticio, sin costo alguno. Debe comunicarse con cada una de las agencias de informes de crédito directamente para obtener dichos informes adicionales