



The HMC Group Marketing, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS4302

29-0008187



[REDACTED]
[REDACTED]
[REDACTED]



July 10, 2026

Subject: Notice of Data Breach

Dear [REDACTED],

We are writing to inform you of a recent data security incident that may have involved your personal information. [REDACTED] takes the privacy and security of all information in our possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information.

What Happened. We recently determined that some of your personal information was involved in a data security incident. We experienced unusual activity involving our computer networks on June 5, 2026, and immediately started an investigation using outside experts to assist. The investigation revealed that some employee personal information could have been accessed or downloaded during the incident. We then worked to determine whose information could have been involved and identify contact information needed to provide notice, which process concluded on June 23, 2026.

What Information Was Involved. The potentially affected information included your [REDACTED]
[REDACTED].

What We Are Doing. As soon as we discovered the incident, we took the steps described above. As part of our ongoing commitment to information security, we are reviewing existing policies and procedures and implementing enhanced security measures to reduce the likelihood of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED] To receive the monitoring services described above, you must enroll within 90

days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity. Please note the deadline to enroll in these services is October 10, 2026.

What You Can Do. You can follow the recommendations on the following page to help protect your information. We also encourage you to take advantage of the complimentary identity protection services being offered.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please contact our dedicated team at **833-851-9637**, Monday through Friday from 5:00 am - 5:00 pm Pacific Time.

Please be assured that [REDACTED] takes the privacy and security of all information within our possession very seriously. We hope you will accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

[REDACTED]
13138 S Bethel Ave
Kingsburg, CA 93631

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

The HMC Group Marketing, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

[REDACTED]
[REDACTED]
[REDACTED]

10 de julio de 2026

Asunto: Aviso de filtración de datos

Estimado(a) [REDACTED]:

Le escribimos para informarle de un reciente incidente de seguridad de datos que puede haber involucrado su información personal. [REDACTED] se toma muy en serio la privacidad y la seguridad de toda la información que tenemos en nuestro poder. Lea esta carta detenidamente, ya que contiene información sobre el incidente y las medidas que puede tomar para ayudar a proteger su información.

Qué sucedió. Recientemente, determinamos que parte de su información personal estuvo involucrada en un incidente de seguridad de datos. El 5 de junio de 2026 experimentamos una actividad inusual en nuestras redes informáticas e inmediatamente iniciamos una investigación con expertos externos que nos ayudaran. La investigación reveló que se pudo haber accedido a parte de la información personal de los empleados o se pudo haber descargado durante el incidente. Posteriormente, trabajamos para determinar de quién podría haberse visto involucrada la información e identificar la información de contacto necesaria para notificar al respecto, cuyo proceso concluyó el 23 de junio de 2026.

Qué información se vio afectada. La información potencialmente afectada incluía su nombre, f [REDACTED]
[REDACTED].

Lo que estamos haciendo. Tan pronto como descubrimos el incidente, tomamos las medidas descritas anteriormente. Como parte de nuestro compromiso continuo con la seguridad de la información, estamos revisando las políticas y los procedimientos existentes, e implementando medidas de seguridad mejoradas para reducir la probabilidad de que ocurra un incidente similar en el futuro. Además, le estamos notificando sobre este evento y le estamos informando sobre los pasos que puede tomar para proteger su información.

Como una precaución adicional, le proporcionamos acceso a los servicios de Monitoreo de crédito de oficina única/Informe de crédito de oficina única/Puntuación de crédito de oficina única sin cargo. Estos servicios le proporcionarán alertas durante 12 meses, a partir de la fecha de inscripción, cuando se produzcan cambios en su archivo de crédito. Esta notificación se le enviaría el mismo día en que se realice el cambio o la actualización con la oficina. Por último, le proporcionaremos asistencia proactiva contra el fraude para ayudarle con cualquier pregunta que pueda tener o en caso de que sea víctima de fraude. Estos servicios se ofrecerán a través de Cyberscout, una empresa de TransUnion que se especializa en servicios de asistencia y remediación de fraudes.



0008187

Para inscribirse en los servicios de Monitoreo de crédito sin cargo, inicie sesión en <https://bfs.cyberscout.com/activate> y siga las instrucciones que se indican. Cuando se le solicite, proporcione el siguiente código único para recibir servicios: [REDACTED]. Para recibir los servicios de monitoreo descritos anteriormente, debe inscribirse dentro de los 90 días a partir de la fecha de esta carta. La inscripción requiere una conexión a Internet y una cuenta de correo electrónico, y es posible que no esté disponible para menores de 18 años. Tenga en cuenta que al inscribirse en los servicios de monitoreo, es posible que se le pida que verifique su información personal para su propia protección a fin de confirmar su identidad. Tenga en cuenta que la fecha límite para inscribirse en estos servicios es el 10 de octubre de 2026.

Qué puede hacer. Puede seguir las recomendaciones de la página siguiente para ayudar a proteger su información. También le recomendamos que aproveche los servicios de protección de identidad de cortesía que se ofrecen.

Para obtener más información. En la página siguiente, encontrará más información sobre cómo proteger su información personal. Si tiene preguntas o necesita ayuda, comuníquese con nuestro equipo dedicado al **833-851-9637**, de lunes a viernes, de 5:00 a. m. a 5:00 p. m., hora del Pacífico.

Tenga en cuenta que [REDACTED] se toma muy en serio la privacidad y la seguridad de toda la información que tenemos en nuestro poder. Esperamos que acepte nuestras más sinceras disculpas y sepa que lamentamos profundamente cualquier preocupación o inconveniente que esto pueda causarle.

Atentamente,

[REDACTED]
13138 S Bethel Ave
Kingsburg, CA 93631

Medidas que puede tomar para proteger su información personal

Revise sus estados de cuenta y notifique a las fuerzas del orden público sobre actividades sospechosas: Como medida de precaución, le recomendamos que permanezca atento y revise detenidamente sus estados de cuenta e informes de crédito. Si detecta alguna actividad sospechosa en una cuenta, debe notificar de inmediato a la institución financiera o a la empresa en la que tiene la cuenta. También debe informar de inmediato cualquier actividad fraudulenta o caso presunto de robo de identidad a las fuerzas del orden público pertinentes, al fiscal general del estado o a la Comisión Federal de Comercio (Federal Trade Commission, FTC).

Copia del informe de crédito: Puede obtener una copia gratuita de su informe de crédito de cada una de las tres agencias principales de informes de crédito cada 12 meses. Para ello, debe visitar www.annualcreditreport.com, llamar al número gratuito 1-877-322-8228 o completar un Formulario de solicitud de informe de crédito anual y enviarlo por correo postal a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. También puede comunicarse con una de las siguientes tres agencias nacionales de informes de crédito:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Alerta de fraude: Le recomendamos que establezca una alerta de fraude en su informe de crédito. La alerta de fraude inicial es gratuita y permanece en su archivo de crédito durante al menos un año. La alerta informa a los acreedores sobre posibles actividades fraudulentas en su informe y les solicita que se comuniquen con usted antes de crear cuentas a su nombre. Para establecer una alerta de fraude en su informe de crédito, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas anteriormente. Puede encontrar información adicional en www.annualcreditreport.com. En TransUnion: www.transunion.com/fraud-alerts.

Congelamiento de seguridad: Tiene derecho a establecer un congelamiento de seguridad en su archivo de crédito durante un máximo de un año sin costo alguno. Esto evitará que se obtenga un crédito nuevo a su nombre sin el uso de un número de identificación personal (Personal Identification Number, PIN) que se le emite cuando inicia el congelamiento. Un congelamiento de seguridad está diseñado para evitar que los posibles acreedores accedan a su informe de crédito sin su consentimiento. Como resultado, el uso de un congelamiento de seguridad puede obstaculizar o retrasar su capacidad de obtener crédito. Debe establecer un congelamiento de seguridad en su archivo de crédito por separado con cada agencia de informes de crédito. Para establecer un congelamiento de seguridad, es posible que deba proporcionar a la agencia de informes del consumidor información que le identifique, como su nombre completo, número de Seguro Social, fecha de nacimiento, direcciones actuales y anteriores, una copia de su tarjeta de identificación emitida por el estado y una factura de servicios públicos, estado de cuenta bancario o estado de cuenta de seguro recientes. En TransUnion: www.transunion.com/credit-freeze.

Recursos gratuitos adicionales: Puede obtener información de las agencias de informes del consumidor, la FTC o el fiscal general del estado respectivo sobre alertas de fraude, congelamientos de seguridad y medidas que puede tomar para prevenir el robo de identidad. Puede informar un presunto robo de identidad a las fuerzas locales del orden público, incluida la FTC o el fiscal general del estado.

Comisión Federal de Comercio

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Fiscal general de California

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

También tiene ciertos derechos en virtud de la Ley Federal de Informes de Crédito Justos (Fair Credit Reporting Act, FCRA): Estos derechos incluyen saber qué consta en su archivo, disputar información incompleta o inexacta, exigir que las agencias de informes del consumidor corrijan o eliminen información inexacta, incompleta o no verificable, entre otros derechos. Para obtener más información sobre la FCRA y sus derechos en virtud de esta ley, visite www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.