

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MICHAEL J. BONNER
mbonner@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Visit us online at
www.C-WLAW.com

DIANNA M. HALL
dhall@c-wlaw.com

Telephone: (610) 567-0700
Fax: (610) 567-0712

August 2, 2022

Via E-Mail

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202
Idtheft@oag.state.md.us

RE: Data Breach Notification

To Whom It May Concern:

We serve as counsel for Your Business, Inc. ("Your Business"), located at P.O. Box 427, Woodland Hills, CA 91365. We write to provide notification of a recent data breach. By providing this notice, Your Business does not waive any rights or defenses under Maryland law, including the data breach notification statute.

Your Business recently learned that certain payment cards used to purchase products on a portion of its website may have been accessed by an unauthorized individual. Your Business immediately began an investigation, which included working with third-party specialists. The investigation determined that an unauthorized individual used malware placed on the Your Business website to obtain payment card data for certain purchases made on the website between April 23, 2022 and May 31, 2022. On July 18, 2022, Your Business confirmed the individuals who made purchases on the website during that time period.

Your Business identified personal information related to the one Maryland resident who may have been impacted by this incident. The information potentially impacted included first and last name and payment card information.

In response to this incident, Your Business conducted an investigation, notified its payment processor, and changed its third-party vendor associated with this incident. Additionally, Your Business began providing notice to the potentially impacted individuals on July 29, 2022. A copy of the notice is attached as ***Exhibit A***. In an abundance of caution, Your Business is offering the potentially impacted individuals complimentary credit monitoring and identity protection services for 12 months.

Please contact me should you have any questions.

Very truly yours,



Michael J. Bonner, Esq.
CIPRIANI & WERNER, P.C.
Counsel for Your Business, Inc.

EXHIBIT A



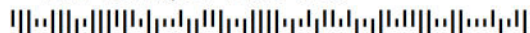
P.O. Box 427
Woodland Hills, CA 91365

August 2, 2022

i1643-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 CA - CT - GENERAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



[Variable Heading (English)]

Dear Sample A. Sample:

As you are well aware, cyber incidents are one of the most common misdeeds in current times. Many major corporations, government agencies, and many of us individually have had to face one of these uncomfortable situations. I regret that I must write to you about an unfortunate incident that may affect the security of payment card information used to make purchases through our website. I assure you we are taking this incident seriously and we are providing you information about the incident, our response, and steps you can take to help protect yourself.

I would also like to take this opportunity to ask you to join me with your cleaning with this situation that unfortunately looks like is so common these days.

What Happened? We recently learned that certain payment cards used to purchase our products on a portion of our e-commerce website may have been accessed by an unauthorized individual outside our organization. We immediately began an investigation, which included working with third-party specialists. Our investigation determined that an unauthorized individual used malware placed on our website to obtain payment card data for certain purchases made on our website between April 23, 2022 and May 31, 2022. On July 18, 2022, we determined you made a purchase on our website during that time period.

What Information Was Involved? The type of information contained on the payment form may include your name, phone number, email address, mailing/billing address, payment card number, expiration date, and CID/CVV number.

What Are We Doing? We conducted an investigation to determine the cause of this incident and also changed our third-party vendor associated with this incident. Additionally, in an abundance of caution, we are providing potentially impacted individuals access to ## months of credit monitoring and identity protection services at no cost to you.

What Can You Do? We encourage you to enroll in the credit monitoring and identity protection services we are making available to you. Information about how to enroll in these services and additional services available to you are included in the enclosed *Steps You Can Take to Help Protect Your Information*.

0000001



i1643-L01



P.O. Box 427
Woodland Hills, CA 91365

2 de agosto de 2022

SAMPLE A SAMPLE - L01 CA - CT - General
123 ANY STREET
APT ABC
ANYTOWN, ST 12345-6789

[Variable Heading (Spanish)]

Estimado/a Sample A. Sample:

Hoy en día, los incidentes en Internet son un problema común y los delitos cibernéticos son cada vez más frecuentes. La mayoría de las grandes corporaciones, las agencias gubernamentales, y muchos de nosotros de forma particular, hemos tenido que enfrentar una de estas situaciones incómodas alguna vez. Lamentablemente, nosotros no hemos sido la excepción y por esta razón te escribimos este mensaje para informarte sobre un incidente que tuvimos y que pudo haber afectado la seguridad de la información de tu tarjeta de compras que has utilizado en nuestro sitio web. Quiero asegurarte que estamos tomando seriamente esta situación y, además de estar brindando toda la información sobre el incidente, también estamos aconsejando sobre los pasos de seguridad que te recomendamos tomar desde ahora para proteger tus datos.

También, quisiera aprovechar esta oportunidad para pedirte que me acompañes en la limpieza con esta situación que últimamente parece ser tan común.

¿Qué pasó? Recientemente nos enteramos de que ciertas tarjetas de compra, tanto de débito y crédito, utilizadas para comprar productos en la sección de comercio electrónico de nuestro sitio web, pudieron haber sido copiadas por una persona no autorizada fuera de nuestra organización. Por esta razón, inmediatamente contratamos a un equipo especializado en seguridad informática que realizó una exhaustiva investigación y que determinó que, efectivamente, una persona no autorizada colocó malware (un programa malicioso) en nuestro sitio web para obtener datos de tarjetas de pago para las compras realizadas entre el 23 de abril de 2022 y el 31 de mayo de 2022. Después de exhaustivas investigaciones, en los reportes finales obtenidos el 18 de julio de 2022 detectamos que tú realizaste una compra en nuestro sitio web durante el período de tiempo afectado y por esta razón queríamos darte aviso del incidente para tu seguridad.

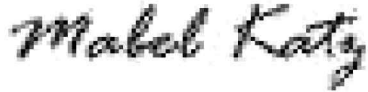
¿Qué información se involucró? El tipo de información contenida en el formulario de pago podría incluir tu nombre, número de teléfono, dirección de correo electrónico, dirección postal y de facturación, número de tarjeta de pago, fecha de vencimiento y número CID / CVV (código de seguridad).

¿Qué estamos haciendo? Llevamos a cabo una investigación exhaustiva para determinar la causa del incidente y también cambiamos nuestro proveedor de hosting externo asociado al incidente. Además, extremando las medidas de precaución, estamos proporcionando a las personas potencialmente afectadas acceso a ## meses de servicios de monitoreo y protección de identidad sin costo alguno.

For More Information: We understand you may have questions about this incident. You may leave us a message at (818) 704-8195, or write to us at support@mabelkatz.com or Your Business Inc, PO Box 427, Woodland Hills, CA 91365. We will get back to you as soon as we can.

We greatly appreciate your business and remain committed to taking the necessary steps to further protect information provided to us.

Sincerely,

A handwritten signature in black ink that reads "Mabel Katz". The script is cursive and fluid, with the first letters of each word being capitalized and prominent.

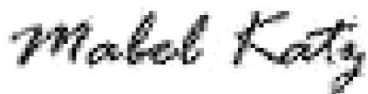
Mabel Katz
President, Your Business, Inc.



¿Qué puedes hacer? Te recomendamos que te inscribas inmediatamente en los servicios de monitoreo y protección de identidad que desde ahora ponemos a tu disposición. La información sobre cómo inscribirse en estos servicios se incluye en el anexo que adjuntamos a este mensaje titulado: *Pasos sugeridos para ayudarte a proteger tu información*.

Para obtener más información: Entendemos que puedes tener muchas inquietudes y preguntas sobre este incidente. De ser así puedes comunicarte con nosotros al +1 818-704-8195, escribirnos a support@mabelkatz.com o a Your Business, Inc., PO Box 427, Woodland Hills, CA 91365. Te responderemos tan pronto nos sea posible. Apreciamos enormemente tu comprensión y te informamos que estamos totalmente comprometidos a tomar todas las medidas necesarias para proteger cualquier información que se nos proporciona.

Sinceramente,

A handwritten signature in black ink that reads "Mabel Katz". The script is cursive and fluid, with the first letters of each word being capitalized and prominent.

Mabel Katz
Presidente
Your Business, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring and Identity Protection Services from Experian

We are offering you access to ## months of credit monitoring and identity protection services from Experian. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: **October 31, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **<https://www.experianidworks.com/credit>**
- Provide your activation code: **ABCDEFGHI**

Additional Details Regarding Your Experian IdentityWorks Membership:

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. Terms and conditions apply.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or

0000001



PASOS SUGERIDOS PARA AYUDARTE A PROTEGER TU INFORMACIÓN

Inscríbete en los servicios de supervisión y protección de identidad de Experian

Te ofrecemos acceso a ## meses de servicios de monitoreo y protección de identidad de Experian. Para comenzar a monitorear tu información personal, siga los pasos a continuación:

- Asegúrete de inscribirte antes del: **31 de octubre de 2022** (tu código no funcionará después de esta fecha).
- Visita el sitio web de Experian IdentityWorks, Puedes inscribirte aquí:
<https://www.experianidworks.com/credit>
- Ingresa este código de activación: **ABCDEFGHI**

Detalles adicionales sobre tu membresía de Experian IdentityWorks:

No se requiere una tarjeta de crédito para inscribirse en Experian IdentityWorks. Puedes ponerte en contacto con Experian inmediatamente en relación con cualquier problema de fraude y tener acceso a las siguientes funciones una vez que te inscribas en Experian IdentityWorks:

1. **Informe de crédito de Experian al registrarte:** ve qué información está asociada con tu archivo de crédito. Los informes de crédito diarios están disponibles solo para miembros en línea.
2. **Monitoreo de crédito:** Monitorea activamente el archivo de Experian en busca de indicadores de fraude.
3. **Restauración de identidad:** Los especialistas en restauración de identidad están disponibles de inmediato para ayudarte a solucionar el fraude relacionado con el crédito.
4. **Experian IdentityWorks ExtendCARE™:** Recibirás el mismo alto nivel de apoyo de restauración de identidad incluso después de que haya expirado tu membresía de Experian IdentityWorks.
5. **Seguro de robo de identidad de \$1 millón:** Proporciona cobertura para ciertos costos y transferencias electrónicas de fondos no autorizadas. Se aplican términos y condiciones.

Supervisa tus cuentas

Te recomendamos estar atento ante cualquier incidente de robo de identidad y fraude revisando tus informes de crédito y estados de cuenta para detectar actividades sospechosas y errores. Bajo la ley de Estados Unidos de América, tienes derecho a un informe crediticio anual de forma gratuita que puede ser proporcionado por cualquiera de las tres principales agencias de informes de crédito: TransUnion, Experian y Equifax. Para solicitar tu informe de crédito gratuito, visita www.annualcreditreport.com o llama al 1-877-322-8228. Una vez que recibas tu informe de crédito, revísalo buscando cualquier discrepancia e identificando cualquier cuenta que no hayas abierto tú, como también consultas de acreedores que no hayas autorizado. Si tienes preguntas o notas alguna información incorrecta, comunícate con la agencia de informes de crédito.

Además, tienes derecho de colocar una "alerta de fraude" inicial o extendida en un archivo de crédito sin costo alguno. Una alerta de fraude inicial es una alerta anual que se coloca en el archivo de crédito del consumidor. Al ver una alerta de fraude, se requiere que una empresa tome medidas para verificar la identidad del consumidor antes de extender un nuevo crédito. Si eres víctima de robo de identidad, tienes derecho a una alerta de fraude extendida que dura siete años. Si deseas colocar una alerta de fraude, comunícate con cualquiera de las tres agencias de informes de crédito que mencionamos más abajo.

Como alternativa a las alertas de fraude, tienes también el derecho de colocar un "congelamiento de crédito" en un informe de crédito, lo que prohibirá que una agencia de crédito divulgue información en el informe de crédito sin tu autorización expresa. El congelamiento de crédito está pensado para evitar que el crédito, los préstamos y los servicios sean aprobados en tu nombre sin tu consentimiento. Sin embargo, debes tener en cuenta que el uso de un congelamiento de crédito puede retrasar, interferir o prohibir la aprobación de cualquier solicitud posterior o solicitud que hagas con respecto a un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta que implique la extensión de crédito. De conformidad con la ley federal, no se te puede cobrar por colocar o levantar un congelamiento de crédito en tu informe de crédito. Para solicitar un congelamiento de crédito, deberás proporcionar la siguiente información:

1. Nombre completo (incluyendo la inicial del medio, así como también Jr., Sr., III, etc.);
2. Número de Seguro Social;

- identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Your Business, Inc. may be contacted at P.O. Box 427, Woodland Hills, CA 91365.

For 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.



3. Fecha de nacimiento;
4. Domicilio de dos a cinco años anteriores;
5. Comprobante de dirección actual, como una factura de servicios públicos o teléfono;
6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (por ejemplo, licencia de conducir estatal o tarjeta de identificación); y
7. Una copia del informe policial, el informe de investigación o la queja a una agencia de aplicación de la ley sobre el robo de identidad, si eres víctima de robo de identidad.

Si deseas colocar una alerta de fraude o congelación de crédito, comunícate con las tres principales agencias de informes de crédito que se enumeran a continuación:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Información Adicional

Puedes informarte aún más sobre el robo de identidad, las alertas de fraude, los congelamientos de crédito y los pasos que puedes tomar para proteger tu información personal comunicándote con las agencias de informes de crédito, la Comisión Federal de Comercio (FTC), o el Fiscal General de tu estado. La FTC también recomienda presentar una queja ante ellos si se descubre que su información ha sido mal utilizada. Puedes contactar a la FTC en 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. Tienes derecho a presentar un informe policial si alguna vez te has visto afectado por robo de identidad o fraude. Ten en cuenta que para presentar un informe ante la policía por robo de identidad, es probable que debas proporcionar alguna prueba de que has sido víctima. Los casos de robo de identidad conocida o sospechada también deben ser reportado a la policía, al Fiscal General de su estado y a la FTC.

Para los residentes de Maryland, se puede contactar al Fiscal General de Maryland en 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; y www.oag.state.md.us. Your Business, Inc. puede ser contactado en P.O. Box 427, Woodland Hills, CA 91365.

Para los residentes de Nuevo México, tienes derechos de conformidad con la Ley de Informes de Crédito Justos, como el derecho a que se le diga si la información en tu archivo de crédito se ha utilizado en tu contra, el derecho a saber qué hay en tu archivo de crédito, el derecho a solicitar tu puntaje de crédito y el derecho a disputar información incompleta o inexacta. Además, de conformidad con la Ley de Informes de Crédito Justos: (i) las agencias de informes del consumidor deben corregir o eliminar información inexacta, incompleta o no verificable; (ii) las agencias de información al consumidor no pueden reportar información negativa obsoleta; (iii) el acceso a tu archivo es limitado; (iv) debes dar tu consentimiento para que te proporcionen informes de crédito a los empleadores; (v) puedes limitar las ofertas "preseleccionadas" de crédito y seguro que obtengas en función de la información de tu informe de crédito; (vi) y puedes solicitar daños y perjuicios a los infractores. Es posible que tengas derechos adicionales bajo la Ley de Informes de Crédito Justos no mencionados. Las víctimas de robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos de conformidad con la Ley de Informes de Crédito Justos. Te recomendamos que revises tus derechos de conformidad con la Ley de Informes de Crédito Justos visitando https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o escribiendo al Centro de Respuesta al Consumidor, Sala 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

Para los residentes de Carolina del Norte, el Fiscal General de Carolina del Norte puede ser contactado en 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 o 1-919-716-6000; y www.ncdoj.gov.