CITY OF
OXNARD
CALIFORNIA

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Notice of Data Breach

<<Date>>

Dear <<Name 1>>:

The City of Oxnard takes seriously the security and protection of its customers' confidential information. The city was recently alerted about unauthorized charges on credit cards used by customers who paid their utility bills online.

The following information outlines what happened, what the city has done in response and steps customers can take to protect their information.

What Happened

On May 22, 2018, the city received a call from a banking institution advising that some of their credit card holders experienced fraudulent purchases on their accounts and these were the same cards used to pay their City of Oxnard utility bills with its Click2Gov (Superion) online payment system.

Upon discovery, the City immediately reported the issue to the Police Department and Superion, which engaged a third-party forensic firm to determine what happened and what information may have been affected. Superion alerted the City to a software vulnerability that had the potential to allow an unauthorized individual to gain access to the computer used to process credit card transactions.

Security patches were applied by Superion on a new server to eliminate the vulnerability with the thought that the issue was resolved. On May 29, 2018, Superion informed the City of additional security controls that were required to secure the system. The City shut down the system immediately so these security controls could be implemented. Even though the vendor's investigation could not specifically confirm or verify the exact method by which any credit card data could have been compromised, the City has decided to notify customers out of an abundance of caution.

What Information Was Involved

The City's vendor has indicated that this incident may affect only individuals who used the City's Click2Gov payment system to make a payment of their City of Oxnard utility bill between March 25 and May 29, 2018. The unauthorized user may have accessed information that included customer names, billing addresses, payment card numbers, CVVs (security code) and expiration dates.

Customers who pay utility bills over the phone with the interactive voice response system and those that have set-up automatic payments are not impacted by this incident, since that is a separate system.

What We Are Doing

The City of Oxnard is working to address this issue and has taken the actions noted above. To help prevent a similar incident in the future, the City is taking steps to enhance its existing security protocols and is working with its vendors to improve protection of personal information in its payment systems.

What You Can Do

Customers should review their payment card account statements closely and report any unauthorized charges to their card issuer immediately because card-network rules generally provide that cardholders are not responsible for unauthorized charges that are reported promptly. The phone number to call is usually on the back of the payment card. If your financial institution requires a police report, please go to www.oxnardpd.org.

For More Information

For more information about fraud and identity theft, visit: www.oxnardpd.org/fraud. You should also review the additional information on the following page on ways to protect yourself. Your confidence and trust are important, and the city apologizes for and deeply regrets any inconvenience or concern this may cause.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted] This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

Sincerely,

[redacted]

Jesús Nava
Interim City Manager

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580,
1 -877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit granters from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit-reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit-reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order 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, provide the addresses where you have lived over the prior five years.
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. 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.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit-reporting agencies by mail and include proper identification (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 identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days 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 send a written request to each of the three credit bureaus by mail and include 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 three (3) business days after receiving your request to remove the security freeze.

CITY OF
OXNARD
CALIFORNIA

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

Notificación sobre violación de datos

<<Date>>

Estimado <<Name 1>>:

La ciudad de Oxnard toma en serio la seguridad y protección de la información confidencial de sus clientes. La ciudad hace poco recibió un alerta acerca de cargos no autorizados en tarjetas de crédito usadas por los clientes para pagar sus facturas de servicios públicos.

La siguiente información describe lo que sucedió, lo que la ciudad ha hecho en respuesta y pasos que los clientes pueden tomar para proteger su información.

Qué ocurrió

El 22 de mayo de 2018, la ciudad recibió una llamada de una institución bancaria para informar que algunos de sus sostenedores de la tarjeta de crédito experimentaron compras fraudulentas en sus cuentas, y eran las mismas tarjetas utilizadas para pagar sus cuentas de la utilidad de la ciudad de Oxnard con su Click2Gov (Superion) sistema de pago en línea.

Tras el descubrimiento, la ciudad informó inmediatamente de la cuestión al Departamento de policía y Superion, quienes contrataron a una empresa forense externa para determinar qué sucedió y qué información se pudo haber afectado. Superion alertó a la ciudad acerca de una vulnerabilidad del software que tenía el potencial de permitir a un individuo no autorizado a tener acceso a la computadora utilizada para procesar las operaciones con tarjeta de crédito.

Los parches de seguridad fueron aplicados por Superion el proveedor de la ciudad en un nuevo servidor para eliminar la vulnerabilidad con el pensamiento de que el problema se resolvió. El 29 de mayo de 2018, el vendedor de la ciudad informó a la ciudad de los controles de seguridad adicionales que se requirieron para asegurar el sistema. La ciudad cerró el sistema inmediatamente para que estos controles de seguridad pudieran ser implementados. A pesar de que la investigación del proveedor no pudo confirmar o verificar específicamente el método exacto por el cual cualquier dato de tarjeta de crédito podría haber sido comprometido, la ciudad decidió notificar a los clientes como una precaución.

Qué información estuvo involucrada

El proveedor de la ciudad ha indicado que este incidente puede afectar solamente a los individuos que utilizaron el sistema de pago Click2Gov de la ciudad para hacer un pago de su cuenta de la utilidad de la ciudad de oxnard entre el 25 de marzo y el 29 de mayo de 2018. Es posible que el usuario no autorizado haya accedido a información que incluía los nombres de clientes, domicilios de facturación, el número de la tarjeta de pago, códigos de validación de a tarjeta (Card Verification Value, CVV) (código de seguridad) y las fechas de vencimiento.

Los clientes que pagan facturas de servicios públicos por teléfono con el sistema interactivo de respuesta de voz interactivo no se ven afectados por este incidente, ya que es un sistema separado.

Qué haremos

La ciudad de Oxnard está trabajando para abordar este tema y ha tomado las medidas antes mencionadas anteriormente. Para ayudar a prevenir un incidente similar en el futuro, la ciudad está tomando medidas para mejorar sus protocolos de seguridad existentes y está trabajando con sus proveedores para mejorar la protección de la información personal existente en sus sistemas de pago.

Qué puede hacer usted

Los clientes deben revisar de cerca sus Estado de cuenta de la tarjeta de pago y reportar cualquier cargo no autorizado a su emisor de tarjeta inmediatamente porque las reglas de la red de tarjetas generalmente proveen que los tarjetahabientes no son responsables por cargos no autorizados que son reportan de inmediato. El número de teléfono al llamar está generalmente en la parte posterior de la tarjeta de pago. Si su entidad financiera exige un denuncia policial, ingrese a www.oxnardpd.org.

Para obtener más información

Para más información sobre fraude y robo de identidad, visite: https://www.oxnardpd.org/fraud. También le aconsejamos que revise la información adicional en la siguiente página sobre formas de protegerse. Su seguridad y confianza son importantes para nosotros, y la ciudad lamenta profundamente los inconvenientes o las preocupaciones que esto puede ocasionarle, por lo que ofrece disculpas.

Si tiene más preguntas sobre este incidente, llame a la línea telefónica exclusiva y confidencial gratuita que hemos establecido para responder preguntas al [redacted] Esta línea de respuesta cuenta con profesionales familiarizados con este incidente e informados acerca de lo que usted puede hacer para ayudar a proteger la cuenta en contra de un posible uso indebido de su información. La línea de respuesta está disponible de lunes a viernes, de 6:00 a. m. a 6:00 p. m., hora del Pacífico.

Atentamente.

[redacted]

Jesús Nava
Administrador Interino de la ciudad

MÁS INFORMACIÓN SOBRE FORMAS DE PROTEGERSE

Le recordamos que permanezca vigilante por incidentes de fraude y robo de identidad, y que revise sus estados de cuenta e informes crediticios sin cargo en busca de cualquier actividad no autorizada. Puede obtener una copia de su informe crediticio, sin cargo, una vez cada 12 meses de cada una de las tres compañías de informes crediticios que operan a nivel nacional. Para solicitar su informe crediticio anual gratis, visite www.annualcreditreport.com o llame al número gratuito 1-877-322-8228. La información de contacto de las tres compañías de informes crediticios que operan a nivel nacional es la siguiente:

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Si cree que ha sido víctima de un robo de identidad o tiene motivos para creer que se ha utilizado su información personal sin autorización, comuníquese de inmediato con la Comisión Federal de Comercio y/o con la oficina del Procurador General de su estado. Puede obtener información de estas fuentes acerca de lo que puede hacer una persona para evitar el robo de identidad, así como información sobre las alertas de fraude y los bloqueos de seguridad. También le aconsejamos que se comunique con sus autoridades de aplicación locales y que presente una denuncia policial. Pida una copia de la denuncia policial en caso de que le soliciten que proporcione copias a los acreedores para corregir sus registros. La información de contacto de la Comisión Federal de Comercio es la siguiente:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Alertas de fraude: Existen dos tipos de alertas de fraude que puede colocar en su informe crediticio para avisarles a sus acreedores que podría haber sido víctima de fraude: una alerta inicial y una alerta extendida. Puede solicitar que se coloque una alerta de fraude inicial en su informe crediticio si sospecha que ha sido o está a punto de convertirse en víctima de un robo de identidad. Una alerta de fraude inicial permanece en su informe crediticio durante al menos 90 días. Usted, puede tener una alerta extendida colocada en su informe crediticio si ya ha sido víctima de un robo de identidad y cuenta con la prueba documental pertinente. Una alerta de fraude extendida permanece en su informe crediticio durante siete años. Puede colocar una alerta de fraude en su informe crediticio comunicándose con cualquiera de las tres agencias de informes crediticios nacionales.

Bloqueos crediticios: Usted puede tener derecho a que se coloque un bloqueo crediticio, también llamado bloqueo de seguridad, en su legajo de crédito, para que no se puedan abrir créditos nuevos a su nombre sin el uso de un número PIN que se le emite cuando inicia un bloqueo. Un bloqueo crediticio tiene por objeto evitar que las posibles entidades que podrían otorgarle crédito accedan a su informe crediticio sin su consentimiento. Si coloca un bloqueo crediticio, los posibles acreedores y otros terceros no podrán acceder a su informe crediticio, a menos que suspenda temporalmente el bloqueo. Por lo tanto, el uso de un bloqueo crediticio puede dilatar su capacidad de obtener crédito. Además, se le podrían cobrar cargos para colocar, suspender y/o eliminar un bloqueo crediticio. Las leyes en materia de bloqueo crediticio varían según el estado. El costo de colocación, suspensión temporal y eliminación de un bloqueo crediticio también varía según el estado, en general, $5 a $20 por acción en cada compañía de informes crediticios. A diferencia de la alerta de fraude, debe colocar por separado un bloqueo crediticio en su legajo de crédito en cada compañía de informes crediticios. Debido a que las instrucciones sobre cómo establecer un bloqueo crediticio varían según el estado, le recomendamos que se comunique con las tres compañías de informes crediticios más importantes, tal como se indica a continuación, para obtener más información.

Para colocar un bloqueo de seguridad en su informe crediticio, debe enviar una solicitud por escrito a cada una de las tres agencias de informes crediticios más importantes por correo ordinario, certificado o con entrega al día siguiente, a los domicilios que se indican a continuación:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

Para solicitar un bloqueo de seguridad, tendrá que proporcionar la siguiente información:

1. Su nombre completo (incluida 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 ha mudado en los últimos cinco (5) años, proporcione las direcciones donde haya vivido durante los últimos cinco años
5. Prueba del domicilio actual, como por ejemplo, una factura de servicios públicos o una factura de teléfono.
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. Si ha sido víctima de un robo de identidad, incluya una copia de la denuncia policial, del informe de la investigación, o de la denuncia ante un organismo de aplicación por el robo de identidad.

Las agencias de informes crediticios disponen de tres (3) días hábiles después de recibir la solicitud para implementar un bloqueo de seguridad en su informe crediticio. Las agencias de crédito también deben enviarle una confirmación escrita en un plazo de cinco (5) días hábiles y proporcionarle una contraseña o un número de identificación personal (Personal Identification Number, PIN) único, o ambos, que puede utilizar para autorizar la eliminación o suspensión del bloqueo de seguridad.

Para suspender el bloqueo de seguridad con el fin de permitir que una entidad o persona específica acceda a su informe crediticio, debe llamar o enviar una solicitud escrita por correo a las agencias de informes crediticios e incluir la identificación correspondiente (nombre, dirección y número de seguro social) y el número de PIN o la contraseña que recibió al colocar el bloqueo de seguridad. También debe incluir la identidad de las entidades o personas que desea que reciban su informe crediticio o el plazo específico durante el cual desea que esté disponible. Las agencias de informes crediticios disponen de tres (3) días hábiles después de recibir la solicitud para suspender el bloque crediticio para las entidades identificadas o durante el plazo indicado.

Para eliminar el bloqueo de seguridad, debe enviar una solicitud escrita por correo a cada una de las tres agencias de crédito e incluir la identificación correspondiente (nombre, dirección y número de seguro social) y el número de PIN o la contraseña que recibió al colocar el bloqueo de seguridad. Las agencias de crédito disponen de tres (3) días hábiles luego de recibir su solicitud para eliminar el congelamiento de seguridad.