



Dykema Gossett PLLC

10 S. Wacker Drive
Suite 2300
Chicago, IL 60606

WWW.DYKEMA.COM

Tel: (312) 876-1700

Fax: (312) 876-1155

Matthew Dybas

Direct Dial: (312) 627-2510

Direct Fax: (855) 230-2515

Email: MDybas@dykema.com

November 27, 2019

Sent via email to

attorneygeneral@doj.nh.gov

New Hampshire Department of Justice
Office of Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General Gordon MacDonald:

I represent Crowe PR PSC, a business that provides customers with accounting, auditing, business and tax consulting services. I am sending this letter pursuant to N.H. Rev. Stat. Ann. § 359-C:20. Crowe PR PSC learned that the personal information of a New Hampshire resident had potentially been exposed to an unknown third party following a compromise of an employee's e-mailbox. The incident involved the potential unauthorized access of the following types of data belonging to the New Hampshire resident: name and Social Security number.

As part of our investigation on behalf of Crowe PR PSC, we retained an external forensics consultant to determine what happened and whether any individual's data had been compromised. Crowe PR PSC also informed the Federal Bureau of Investigation of the security incident, but resident notification was not delayed due to a law enforcement investigation. Crowe PR PSC notified the affected individual on October 18, 2019. Further, Crowe PR PSC is providing the individual with 12 months of complimentary identity protection services through MyIDCare, which consists of 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy and fully managed ID theft recovery services. To prevent this type of incident from occurring in the future, Crowe PR PSC is reinforcing existing security protocols and providing additional training to its employees.

A copy of the template notification letter to the affected resident of New Hampshire is enclosed. Please contact me if you have any questions.



New Hampshire Department of Justice
November 27, 2019
Page 2

Very truly yours,

DYKEMA GOSSETT, PLLC

A handwritten signature in blue ink, appearing to read "Matthew Dybas", with a long horizontal flourish extending to the right.

Matthew Dybas



C/O ID Experts
PO Box 4219
Everett WA 98204

To Enroll, Please Call:
(833) 967-1097
Or Visit:
<http://ide.myidcare.com/cprpsc>
Enrollment Code: <<XXXXXXXXXX>>

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

COUNTRY



SEQ
CODE 2D
Ver1CM

BREAK

October 18, 2019

Notice of Data Breach

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

The protection of your personal information is a priority for us at Crowe PR PSC (Crowe). Unfortunately, we are writing to inform you of an incident that occurred potentially involving your personal information. We take this matter very seriously and understand the personal nature of the information at issue, which is why we are offering you the opportunity to enroll in MyIDCare™, a complimentary identity protection service, to reduce the chances of identity theft or fraud on your accounts.

What Happened

On September 18, 2019, we learned that your personal information was potentially impacted as a result of a phishing attack by an unknown third party on an employee’s email account. As part of our investigation, we hired a forensic consultant to determine if any personal information has been exposed as a result of the attack. At this time, there is no evidence to suggest that there has been any attempt to misuse any of your personal information. Out of an abundance of caution, we are taking a number of actions to protect your identity.

What Information Was Involved

Your personal information that was potentially impacted includes your <<Variable Data 2 >>.

What We Are Doing

The privacy and security of your personal information is of the highest importance to us, and we are handling this incident with the greatest of care. In response to the phishing attack, we have notified the FBI of the incident, however, our notification to you was not delayed as a result of a law enforcement investigation. We have also reinforced exiting security protocols to recognize likely phishing schemes and to reduce the likelihood of a similar event occurring in the future, including providing additional training to our employees.

In addition, we are offering identity theft protection services through ID Experts®, a data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We want to stress again that we have no evidence that any of your personal information was misused. We are simply putting every effort into minimizing any impact to you. We recommend you to take full advantage of the services with ID Experts.

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 967-1097 or going to <http://ide.myidcare.com/cprpsc> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9:00 a.m. - 9:00 p.m. Eastern Time. Please note the deadline to enroll is January 18, 2020.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. Representatives can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, 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. We cannot stress enough that the protection of your information is of the utmost importance to us.

Please call (833) 967-1097 or go to <http://ide.myidcare.com/cprpsc> for assistance or for any additional questions you may have. You may also contact Juan Bruno by email at guilobruno@hotmail.com.

Sincerely,

Crowe PR PSC

Crowe PR PSC

(Enclosure)



Recommended Steps To Help Protect Your Information

- 1. Website and Enrollment.** Go to <http://ide.myidcare.com/cprpsc> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at (833) 967-1097 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. 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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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.

5. 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.alerts.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.

6. 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.

7. 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 (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

Iowa Residents: You have the right to report suspected incidents of identity theft to local law enforcement or the Iowa Office of the Attorney General, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, www.iowaattorneygeneral.gov/for-consumers, Telephone: 515-281-6771.

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.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



C/O ID Experts
PO Box 4219
Everett WA 98204

To Enroll, Please Call:
(833) 967-1097
Or Visit:
<http://ide.myidcare.com/cprpsc>
Enrollment Code: <<XXXXXXXXXX>>

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

18 de Octubre de 2019

Notificación de Filtración de Datos

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

La protección de su información personal es una prioridad para Crowe PR PSC (Crowe). Desafortunadamente, le escribimos para informarle de un incidente que posiblemente a afectado su información personal. Nosotros tomamos este asunto muy en serio y entendemos el tipo de información personal en cuestión, es por eso que le ofrecemos la oportunidad de inscribirse en MyIDCare™, un servicio gratuito de protección de identidad, para reducir las posibilidades de robo de identidad o fraude en sus cuentas.

¿Qué ocurrió?

El 18 de septiembre de 2019, nos enteramos de que su información potencialmente fue afectada como resultado de un ataque de phishing por parte de un tercero desconocido en la cuenta de correo electrónico de nuestro empleado. Como parte de nuestra investigación, contratamos a un consultor forense para determinar si se ha expuesto información personal como resultado del ataque. En este momento, no hay evidencia que sugiera que haya habido algún intento de mal uso de su información personal. Por una abundancia de precaución, estamos tomando una serie de acciones para proteger su identidad.

¿Qué información estuvo involucrada?

Su información personal que potencialmente fue impactada incluye <<Variable Data 3 >>.

¿Qué estamos haciendo?

La privacidad y seguridad de su información personal es de alta importancia para nosotros, y estamos manejando este incidente con el mayor cuidado. En respuesta al ataque de phishing, hemos notificado al FBI del incidente, sin embargo, nuestra notificación a usted no se retrasó como resultado de la investigación policial. También hemos reforzado la salida de protocolos de seguridad existentes para reconocer posibles esquema de phishing y reducir la probabilidad de que ocurra un evento similar en el futuro, incluyendo proporcionar capacitación adicional a nuestros empleados.

Además, ofrecemos servicios de protección contra robo de identidad a través de ID Experts®, un experto en servicios de violación de datos y recuperación, para proporcionarle MyIDCare™. MyIDCare servicios incluyen: 12 meses de monitoreo de Crédito y CyberScan, una póliza de reembolso de seguro de \$1,000,000 y servicios de recuperación de robo de identidad totalmente administrados. Con esta protección, MyIDCare le ayudará a resolver problemas si su identidad se ve comprometida.

Queremos enfatizar nuevamente que no tenemos evidencia de que su información personal haya sido mal utilizada. Simplemente estamos haciendo todo lo posible para minimizar cualquier impacto para usted. Le recomendamos que aproveche al máximo los servicios con ID Experts.

¿Qué puede hacer usted?

Le recomendamos que se ponga en contacto con ID Experts si tiene alguna pregunta y que se inscriba en los servicios gratuitos de MyIDCare llamando al (833) 967-1097 o visitando <http://ide.myidcare.com/cprpsc> y utilizando el Código de inscripción proporcionado anteriormente. Los expertos de MyIDCare están disponibles de lunes a viernes de 9:00 a.m. a 9:00 p.m. hora del este. Tenga en cuenta que la fecha límite para inscribirse es 18 de enero de 2020.

Una vez más, en este momento, no hay evidencia de que su información haya sido mal utilizada. Sin embargo, le recomendamos que aproveche al máximo esta oferta de servicios. Los representantes pueden responder preguntas o inquietudes que pueda tener con respecto a la protección de su información personal.

Para más información

Encontrará instrucciones detalladas para la inscripción en el documento adjunto Pasos recomendados. También, tendrá que hacer referencia al código de inscripción en la parte superior de esta carta al llamar o inscribirse en línea, así que por favor no deseche esta carta. No podemos enfatizar lo suficiente que la protección de su información es de alta importancia para nosotros.

Por favor llame a (833) 967-1097 o visite <http://ide.myidcare.com/cprpsc> para asistencia o para cualquier pregunta adicional que pueda tener. También puede contactar a Juan Bruno por correo electrónico a guilobruno@hotmail.com.

Sinceramente,

Crowe PR PSC

Crowe PR PSC

(Recintos)



Pasos Recomendados para Proteger su Información

- 1. Sitio web e inscripción.** Visite el sitio web <http://ide.myidcare.com/cprpsc> y siga las instrucciones para inscribirse.
- 2. Active el monitoreo de crédito.** Su membresía en MyIDCare incluye el monitoreo de crédito, pero usted debe activarlo personalmente para que tome efecto. Nota: Debe haber establecido crédito y acceso a una computadora y Internet para usar este servicio. Si necesita ayuda, MyIDCare podrá ayudarlo.
- 3. Teléfono.** Comuníquese con MyIDCare llamando a (833) 967-1097 para obtener información adicional sobre este incidente y hable con representantes concedores sobre los pasos apropiados para proteger su identidad crediticia.
- 4. Revise sus informes de crédito.** Como medida de precaución le recomendamos que permanezca atento revisando sus estados de cuenta y informes de crédito. Bajo la ley federal usted tiene derecho a obtener una copia gratuita de su informe de crédito cada 12 meses de cada una de las tres principales compañías de informe de crédito. Para obtener un informe de crédito anual gratuito, visite www.annualcreditreport.com o llame 1-877-322-8228. Es posible que desee escalar sus solicitudes para que reciba un informe gratuito de una de las tres agencias de crédito cada cuatro meses.

Si descubre algún elemento sospechoso y se ha inscrito en MyIDCare, notifíquelo de inmediato llamando o iniciando sesión en el sitio web de MyIDCare y presentando una solicitud de ayuda.

Si presenta una solicitud de ayuda o informa actividades sospechosas, un miembro de nuestro equipo de ID Care se comunicará con usted y lo ayudará a determinar la causa de los elementos sospechosos. En el improbable caso de que usted sea víctima de robo de identidad como consecuencia de este incidente, se le asignará un especialista en atención de identificación que trabajará en su nombre para identificar, detener y revertir el daño rápidamente.

También debe saber que tiene derecho a presentar un informe policial si alguna vez experimenta fraude de identidad. Tenga en cuenta que, con el fin de presentar un informe de delito o de incidente de robo de identidad, es probable que tenga que proporcionar algún tipo de prueba que demuestre que usted ha sido una víctima. A menudo se requiere un informe policial para disputar actos fraudulentos. Usted puede reportar presuntos incidentes de robo de identidad a las autoridades locales de la ley o al Procurador General de los Estados Unidos.

5. Coloque alertas de fraude con las tres agencias de crédito Si opta por colocar una alerta de fraude, le recomendamos que lo haga luego de activar su monitoreo de crédito. Puede colocar una alerta de fraude en una de las tres agencias de crédito principales por teléfono y también a través del sitio web de Experian o Equifax. Una alerta de fraude le indica a los acreedores que sigan ciertos procedimientos, incluido el contacto con usted, antes de que abran cuentas nuevas o cambien sus cuentas existentes. Por esta razón, colocar una alerta de fraude puede protegerle, pero también puede retrasarle cuando usted solicite crédito. La información de contacto de las tres agencias es la siguiente:

Agencias de Crédito

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.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 contactar solo a UNA de estas agencias y usar solo UNO de estos métodos. Tan pronto una de las tres agencias confirme su alerta de fraude, a las demás se les notifica para que coloquen alertas en sus registros también. Recibirá cartas de confirmación por correo y luego podrá ordenar los tres informes de crédito sin cargo para su revisión.

Tenga en cuenta: Nadie puede colocar una alerta de fraude en su informe de crédito, excepto usted.

6. Congelamiento de Seguridad. Al colocar un congelamiento de seguridad, si alguna persona obtiene su información de identificación personal de manera fraudulenta, esta no podrá usar la información para abrir nuevas cuentas o pedir dinero prestado a nombre suyo. Deberá ponerse en contacto por escrito con las tres agencias nacionales de informes de crédito indicadas anteriormente para colocar el congelamiento. Tenga en cuenta que cuando coloque el congelamiento, no podrá pedir dinero prestado, obtener crédito instantáneo u obtener una nueva tarjeta de crédito hasta que levante temporalmente o remueva permanentemente el congelamiento. No hay ningún costo para congelar o descongelar sus archivos de crédito.

7. Información Adicional. Puede obtener información adicional sobre los pasos que puede tomar para evitar el robo de identidad con las siguientes agencias. La Comisión Federal de Comercio también le recomienda a aquellas personas que descubren que su información ha sido utilizada indebidamente que presenten una denuncia con ellos.

Residentes de California: Visite la Oficina de Protección de Privacidad de California (www.privacy.ca.gov) para obtener información adicional sobre protección contra el robo de identidad.

Residentes de Iowa: Tiene derecho a denunciar presuntos incidentes de robo de identidad a las autoridades locales o a la Oficina del Fiscal General de Iowa, División de Protección al Consumidor, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, www.iowaattorneygeneral.gov/for-consumers, Teléfono 515-281-6771.

Residentes de North Carolina: Oficina del Fiscal General de North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Teléfono: 919-716-6400.

Todos los residentes de U.S.: Centro de Información de Robo de Identidad, Comisión Federal de Comercio, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.