August 21, 2024

Michael T. Gibson P.A. (the "Firm") recently experienced a data security incident, and we are providing this notice to potentially affected individuals. The Firm takes measures to protect the personal information it maintains and remains committed to helping affected individuals protect themselves. Please read the below notice for more details and to see what steps you can take to help protect yourself.

What happened?
On approximately July 22, 2024, an unauthorized third party compromised the computer systems of one of the Firm's external IT vendor. This unauthorized party used access provided by this external provider to compromise the Firm's computer systems along with those of several other businesses. On July 22, 2024, the unauthorized party extracted files from the Firm's systems that may have included personally identifiable information. On July 23, these cybercriminals deployed ransomware on the Firm's systems, encrypting most of the Firm's computer network. The Firm reported the incident to law enforcement and has worked diligently to investigate and restore operations and security since the attack.

What information was involved?
The data accessed by the attackers was varied and substantial. In some cases, the information included full names, dates of birth, email addresses, telephone numbers, addresses, a combination of these data, or other data an individual may have provided to the Firm in the past. However, due to the volume of files taken, the Firm cannot determine with certainty the exact scope of personal information the attackers may have extracted. To be safe, if you have provided personal information or data to the Firm in the past, you should assume that your personally identifiable information or data may have been compromised in this incident and take appropriate precautions.

What we are doing
The Firm has taken swift action to restore the functionality and security of its data systems following the attack. We are cooperating with law enforcement investigating the attack. The Firm is also working with outside consultants to strengthen our information security systems to reduce the risk of a similar attack in the future. The Firm has also obtained evidence that indicates the files taken by the unauthorized persons have been deleted, and not retained or used maliciously beyond the attack on the Firm itself.

What you can do
The most important thing you can do in response to this incident is to remain vigilant and secure your financial and other accounts. Whether you have been affected by this specific breach or not, it is important to regularly review personal account statements and credit reports to ensure no unauthorized activity has occurred. Here are a few warning signs to help you determine whether your personal information may have been used by someone else:

- Receiving a bill for services or items you did not purchase
- Being contacted by a debt collector about debt you do not owe
- Seeing collection notices on your credit report that you do not recognize

Malicious actors may try to trick you into giving them more information using the compromised data. If you receive any suspicious communications, particularly regarding financial matters, you should verify the source of these communications before revealing any personal information. If you are threatened by anyone, you should contact law enforcement. If you believe you have been the victim of identity theft, you should also contact law enforcement, your state attorney general, or the Federal Trade Commission ("FTC").

You may want to change your passwords to various online accounts. If you do change your passwords, your new password should be substantially different from your old password to best ensure security. Remember, it is never a good idea to use the same password from work for your personal or household applications.

Additionally, you may also consider placing a security freeze on your credit report, as allowed by state law. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please note that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any request you make for new loans, credit, credit or debit cards, mortgages, employment, housing, or other services.

How to freeze your credit report
To place a security freeze on your credit report, you must contact each of the three major consumer reporting agencies individually: Equifax, Experian, and TransUnion. You can do this online, or in writing. To do this online, you can go to each of these websites and create an account. You will need to set up a user ID and password with each agency. If you prefer to contact the agencies in writing, you can send a security freeze request by regular, certified, or overnight mail to the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion Security Freeze
P.O. Box 6790
Fullerton, CA 92834
1-800-909-8872

In order to request a security freeze in writing, 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. The addresses where you have lived over the past 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 victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you elect to set up a security freeze online, the agencies may instead request an email address and telephone number for identity verification.

Identity theft resources
The Federal Trade Commission (FTC) is located at 600 Pennsylvania Avenue, NW Washington, DC 20580. If you believe you may have been a victim of identity theft, you may file a complaint with the FTC at www.ftc.gov/idtheft or by calling 1-877-ID-THEFT (877-438-4338). You may also consider taking additional steps, which are outlined on the FTC's website: https://www.identitytheft.gov/. Here, you will find resources and a checklist of steps you can take to protect yourself.

State governments also provide resources on protecting yourself against identity theft. Some examples of these resources are listed below.

Florida Attorney General
Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399
1-866-966-7226

California Attorney General
P.O. Box 944255
Sacramento, CA 94244-2550
(800) 952-5225

Texas Attorney General
PO Box 12548
Austin, TX 78711-2548
(800) 621-0508

North Carolina Attorney General
114 West Edenton Street
Raleigh, NC 27603
(919) 716-6400

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
410-576-6300

Oregon Attorney General
1162 Court St. NE
Salem, OR 97301-4096
1-877-877-9392

New York Attorney General
Office of the New York State Attorney General
The Capitol Albany NY 12224-0341
1-800-771-7755

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400

If you would like more information from the Firm, or have any questions, please email Gibsoncybersupport@gibsonjustice.com, call our office at 407-422-4529, or our toll-free number of 855-942-8639, and ask to speak to one of our office administrators, Patty Lopez or Bianca Felices, or write us at 2420 S Lakemont Ave #150, Orlando, FL 32814.

21 de agosto de 2024

Michael T. Gibson PA (la "Empresa") experimentó recientemente un incidente de seguridad de datos y proporcionamos este aviso a las personas potencialmente afectadas. La Firma toma medidas para proteger la información personal que mantiene y mantiene su compromiso de ayudar a las personas afectadas a protegerse. Lea el aviso a continuación para obtener más detalles y ver qué medidas puede tomar para protegerse.

¿Qué pasó?
Aproximadamente el 22 de julio de 2024, un tercero no autorizado comprometió los sistemas informáticos de uno de los proveedores de TI externos de la Firma. Esta parte no autorizada utilizó el acceso proporcionado por este proveedor externo para comprometer los sistemas informáticos de la empresa junto con los de varias otras empresas. El 22 de julio de 2024, la parte no autorizada extrajo archivos de los sistemas de la Firma que pueden haber incluido información de identificación personal. El 23 de julio, estos ciberdelincuentes implementaron ransomware en los sistemas de la empresa, cifrando la mayor parte de la red informática de la empresa. La Firma informó el incidente a las autoridades y ha trabajado diligentemente para investigar y restaurar las operaciones y la seguridad desde el ataque.

¿Qué información estuvo involucrada?
Los datos a los que accedieron los atacantes fueron variados y sustanciales. En algunos casos, la información incluía nombres completos, fechas de nacimiento, direcciones de correo electrónico, números de teléfono, direcciones, una combinación de estos datos u otros datos que un individuo pudo haber proporcionado a la Firma en el pasado. Sin embargo, debido al volumen de archivos tomados, la Firma no puede determinar con certeza el alcance exacto de la información personal que los atacantes pueden haber extraído. Para estar seguro, si ha proporcionado información o datos personales a la Firma en el pasado, debe asumir que su información o datos de identificación personal pueden haber sido comprometidos en este incidente y tomar las precauciones adecuadas.

Que estamos haciendo
La Firma ha tomado medidas rápidas para restaurar la funcionalidad y seguridad de sus sistemas de datos luego del ataque. Estamos cooperando con las autoridades que investigan el ataque. La Firma también está trabajando con consultores externos para fortalecer nuestros sistemas de seguridad de la información y reducir el riesgo de un ataque similar en el futuro. La Firma también ha obtenido evidencia que indica que los archivos tomados por personas no autorizadas han sido eliminados y no retenidos ni utilizados de manera maliciosa más allá del ataque a la Firma misma.

Que puedes hacer
Lo más importante que puede hacer en respuesta a este incidente es permanecer alerta y proteger sus cuentas financieras y de otro tipo. Ya sea que se haya visto afectado por esta infracción específica o no, es importante revisar periódicamente los estados de cuenta personales y los informes crediticios para asegurarse de que no se haya producido ninguna actividad no autorizada. Aquí hay algunas señales de advertencia que le ayudarán a determinar si su información personal puede haber sido utilizada por otra persona:

- Recibir una factura por servicios o artículos que no compró
- Ser contactado por un cobrador de deudas sobre una deuda que usted no debe
- Ver avisos de cobro en su informe de crédito que no reconoce

Los actores malintencionados pueden intentar engañarlo para que les proporcione más información utilizando los datos comprometidos. Si recibe alguna comunicación sospechosa, particularmente en relación con asuntos financieros, debe verificar la fuente de estas comunicaciones antes de revelar cualquier información personal. Si alguien lo amenaza, debe comunicarse con la policía. Si cree que ha sido víctima de robo de identidad, también debe comunicarse con las autoridades, el fiscal general de su estado o la Comisión Federal de Comercio ("FTC").

Es posible que desee cambiar sus contraseñas de varias cuentas en línea. Si cambia sus contraseñas, su nueva contraseña debe ser sustancialmente diferente de su contraseña anterior para garantizar mejor la seguridad. Recuerde, nunca es buena idea utilizar la misma contraseña del trabajo para sus aplicaciones personales o domésticas.

Además, también puede considerar colocar un congelamiento de seguridad en su informe crediticio, según lo permite la ley estatal. Un congelamiento de seguridad prohíbe a una agencia de informes crediticios divulgar cualquier información del informe crediticio de un consumidor sin autorización por escrito. Tenga en cuenta que congelar su informe de crédito puede retrasar, interferir o impedir la aprobación oportuna de cualquier solicitud que realice para nuevos préstamos, tarjetas de crédito, crédito o débito, hipotecas, empleo, vivienda u otros servicios.

Cómo congelar su informe de crédito
Para congelar su informe crediticio por seguridad, debe comunicarse individualmente con cada una de las tres principales agencias de informes del consumidor: Equifax, Experian y TransUnion. Puede hacerlo en línea o por escrito. Para hacer esto en línea, puede ir a cada uno de estos sitios web y crear una cuenta. Deberá configurar una identificación de usuario y una contraseña con cada agencia.

Si prefiere comunicarse con las agencias por escrito, puede enviar una solicitud de congelamiento de seguridad por correo regular, certificado o urgente a las siguientes direcciones:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion Security Freeze
P.O. Box 6790
Fullerton, CA 92834
1-800-909-8872

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

1. Su nombre completo (incluyendo la inicial del segundo nombre, así como Jr., Sr., II, III, etc.)
2. Número de Seguro Social
3. Fecha de nacimiento
4. Las direcciones donde ha vivido durante los últimos cinco años.
5. Comprobante de dirección actual, como una factura de servicios públicos o de teléfono actual.
6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir estatal o tarjeta de identificación, identificación militar, etc.)
7. Si es víctima de robo de identidad, una copia de un informe policial, un informe de investigación o una denuncia ante una agencia policial sobre robo de identidad.

Si elige configurar un congelamiento de seguridad en línea, las agencias pueden solicitar una dirección de correo electrónico y un número de teléfono para verificar la identidad.

Recursos sobre robo de identidad
La Comisión Federal de Comercio (FTC) está ubicada en 600 Pennsylvania Avenue, NW Washington, DC 20580. Si cree que puede haber sido víctima de robo de identidad, puede presentar una queja ante la FTC en www.ftc.gov/idtheft o llamando al 1-877-ID-THEFT (877-438-4338). También puede considerar tomar medidas adicionales, que se describen en el sitio web de la FTC: https://www.identitytheft.gov/. Aquí encontrará recursos y una lista de verificación de los pasos que puede seguir para protegerse.

Los gobiernos estatales también brindan recursos para protegerse contra el robo de identidad. Algunos ejemplos de estos recursos se enumeran a continuación.

Florida Attorney General
Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399
1-866-966-7226

California Attorney General
P.O. Box 944255
Sacramento, CA 94244-2550
(800) 952-5225

Texas Attorney General
PO Box 12548
Austin, TX 78711-2548
(800) 621-0508

North Carolina Attorney General
114 West Edenton Street
Raleigh, NC 27603
(919) 716-6400

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
410-576-6300

Oregon Attorney General
1162 Court St. NE
Salem, OR 97301-4096
1-877-877-9392

New York Attorney General
Office of the New York State Attorney General
The Capitol Albany NY 12224-0341
1-800-771-7755

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400

Si desea obtener más información de la firma o tiene alguna pregunta, envíe un correo electrónico a Gibsoncybersupport@gibsonjustice.com, llame a nuestra oficina al 407-422-4529 o a nuestro número gratuito 855-942-8639 y pida hablar. a uno de los administradores de nuestra oficina, Patty Lopez o Bianca Felices, o escríbanos a 2420 S Lakemont Ave #150, Orlando, FL 32814.