Richard Reiter
914.872.7728 (direct)
Richard.Reiter@wilsonelser.com

April 27, 2021

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Security Incident

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Chatham County, North Carolina ("Chatham") with respect to a data security incident described in more detail below. Chatham takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Description of the Incident.

On or about October 28, 2020, Chatham experienced a ransomware attack that resulted in the exposure of personal information of individuals, including current and former Chatham residents and employees, to an unknown individual who was not authorized to view it. Chatham has since worked diligently to determine exactly what happened and what information was involved as a result of this Incident.

Based on the results of an investigation conducted by third-party forensic vendors, Chatham determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: names; dates of birth; home addresses; phone numbers; social security numbers; health information from current employee personnel files; Department of Social Services ("DSS") files, including names; names of household members, and employer and/or wages connected with DSS forms and notes; Medicaid ID numbers; and medical records pertaining to Child Protective Services. The exact elements of personal information that were exposed as a result of this incident varied per individual.

As of this writing, Chatham has not received any reports of fraud or identity theft related to this matter.

2. Number of Maine residents affected.

Chatham discovered that the incident resulted in the unauthorized exposure of information pertaining to three (3) Maine residents. Notification letters to these individuals will be mailed on April 27, 2021, via First Class Mail. A sample copy of the notification letters sent to Maine residents whose health information may have been compromised is attached as **Exhibit A**. A sample copy of the notification letters sent to Maine residents whose personally identifiable information may have been compromised is attached as **Exhibit C**.

3. Steps taken.

Chatham takes the privacy and security of their information seriously, and has taken steps to protect the privacy and security of potentially impacted individuals' information. Upon discovery of the incident, Chatham informed the North Carolina National Guard as well as Wilson Elser, and with the assistance of third-party cyber-security experts, began an investigation into how the ransomware attacked occurred and what information was compromised. Chatham is committed to ensuring the security of all information in its control, and is taking steps to prevent a similar event from occurring in the future. This includes strengthening its cybersecurity posture. Specifically, Chatham is performing additional hardening of its network, platforms, and software to prevent the future occurrence of any similar data security incidents. Additionally, all notified individuals whose social security number was potentially impacted were offered complimentary identity theft and credit monitoring services for a period of twelve (12) months.

4. Contact information.

Chatham remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Richard.Reiter@wilsonelser.com or (914) 872-7728.

Very truly yours,

WILSON ELSER MOSKOWITZ EDELMAN AND DICKER LLP

Richard Reiter

Richard Reiter

EXHIBIT A

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>
<<Address_1>> <<Address_2>>
<<City>>, <<State>> <<Zip Code>>

April 27, 2021

Dear <<First Name>> <<Last Name>>:

You are receiving this letter because we became aware on or about Tuesday February 9, 2021 that County files containing your personal information were recently released at a publicly accessible website maintained by the cyber threat actor(s) responsible for the October 2020 ransomware attack that affected Chatham County (hereinafter, the Incident). This letter contains information about the Incident, how the Incident may have impacted your personal information, steps we are taking to address the Incident, and actions you can take to safeguard your information.

What Happened

The County of Chatham experienced a ransomware attack in October 2020. During a typical ransomware attack, cybercriminals try to "lock" an organization's digital files in an attempt to get paid for a digital key to unlock the files. Sometimes, as was the case here, the cybercriminals will also acquire files from the organization they have targeted and post those files at a publicly accessible location on the internet, commonly referred to as the "dark web."

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to:

- Your Medicaid ID Number;
- Forms and case notes related to the DSS services you have received that may include your name (including the names of your household members) and/or county case number; and
- Your medical records pertaining to Child Protective Services.

At this time, The County does not have any evidence to indicate that other identifying information, such as your social security number or your driver's license number, were compromised as a result of the Incident.

What We Are Doing

The County's investigation of this incident remains ongoing and we are in close communication with our law enforcement partners on this issue. We have also worked closely with the North Carolina Emergency Management and a third-party information technology forensics firm to determine how the attack occurred in an effort to prevent it from happening again.

What You Can Do

At this time, we are not aware of anyone experiencing fraud as a result of this incident. This incident will have no effect on your eligibility for any public benefits such as Medicaid. If you applied for services, your application would continue to be processed normally. That said, we strongly encourage you to remain vigilant and monitor your account statements and Explanation of Benefits (EOB) for any suspicious activity. We also recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

A call center has been established to assist you. If you have any additional questions, please do not hesitate to call 1-833-903-3648.

Sincerely,

Dan J. LaMontagne, PE
Chatham County Manager

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

A/C IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<Nombre>> <<Segundo nombre>> <<Apellido>> <<Fórmula de tratamiento>>
<<Dirección_1>> <<Dirección_2>>
<<Ciudad>>, <<Estado>> <<Código postal>>

27 de abril de 2021

Estimado/a <<Nombre>> <<Apellido>>:

Le enviamos esta carta porque advertimos que el martes 9 de febrero de 2021, o cerca de esa fecha, se dieron a conocer en un sitio web accesible públicamente los archivos del condado en los que constaba su información personal. Dicho sitio corresponde al ejecutor/es de amenazas cibernéticas responsable/s del ataque de chantaje (*ransomware*) ocurrido en octubre de 2020, el cual afectó al condado de Chatham (en adelante, «el incidente»). En la presente carta se le brinda información sobre el incidente, cómo este puede haber repercutido en su información personal, los pasos que estamos tomando para corregirlo y las medidas que usted puede llevar adelante para proteger sus datos.

Qué ocurrió

El condado de Chatham sufrió un ataque de chantaje en octubre de 2020. Lo que ocurre en este tipo de circunstancias es que los cibercriminales tratan de «bloquear» los archivos digitales de determinada organización con el objetivo de que se les pague a cambio de una clave digital para desbloquearlos. Hay veces en que, como ocurrió en este caso, los cibercriminales obtienen archivos de la organización que atacaron y los publican en ciertos sitios de Internet con acceso público, lo que comúnmente se denomina «Internet profunda».

¿Qué información se vio afectada?

Posiblemente, entre los datos personales que se expusieron se encuentran los siguientes, aunque puede haber habido más:

- su número de Medicaid;
- los formularios y las notas de caso sobre los servicios que le prestó el Departamento de Servicios Sociales (DSS por sus siglas en inglés), como su nombre (así como los de quienes viven con usted) o el número de caso que tiene con el condado; y
- los registros médicos correspondientes a los Servicios de Protección a Menores.

El condado no tiene prueba fehaciente en estos momentos de que otros datos que lo identifiquen, como su número de Seguro Social o licencia de conducir, se hayan visto afectados a raíz del incidente.

Qué estamos haciendo

El condado sigue investigado lo ocurrido y está en estrecha comunicación con las fuerzas del orden público que colaboran con nosotros en referencia a este tema. Además, trabajamos codo a codo con la división de manejo de emergencias de

Carolina del Norte y con una firma de informática forense para establecer cómo se produjo el ataque con el fin de evitar que vuelva a ocurrir.

Qué puede hacer usted

No tenemos conocimiento de que alguien haya sido víctima de fraude como consecuencia del incidente hasta ahora. Lo ocurrido no repercutirá en absoluto en su elegibilidad para recibir beneficios públicos, como Medicaid. Si los solicitó, el pedido se tramitará con normalidad. No obstante, le recomendamos fervientemente que esté alerta y revise los estados de cuenta bancarios y la explicación de los beneficios para ver si hay actividad sospechosa. Además, le sugerimos que lea la siguiente página que contiene información importante sobre las medidas que usted puede tomar para proteger su información personal, tales como implementar alertas por fraude o bloqueos de seguridad.

Para obtener más información

Se dispuso un centro de atención para responder a sus consultas. Si tiene preguntas, no dude en llamar al 1-833-903-3648.

Atentamente,

Ing. Dan J. LaMontagne
Administrador del condado de Chatham

Más información importante

Para los residentes de *Hawái, Míchigan, Misuri, Virginia, Vermont* y *Carolina del Norte*: La legislación estatal recomienda que esté alerta ante casos de incidentes de fraude o robo de la identidad. Para ello, revise si en los extractos de las tarjetas de crédito o en los informes de solvencia se registra actividad no autorizada.

Para los residentes de *Illinois, Iowa, Maryland, Misuri, Carolina del Norte, Oregón* y *Virginia Occidental*:
Por la legislación estatal estamos obligados a informarle que puede obtener un ejemplar sin costo de su informe de solvencia, ya sea que sospeche que hubo actividad no autorizada en su cuenta o no. Puede obtener un ejemplar gratuito de cada una de las tres oficinas crediticias del país. Para solicitarlo, ingrese a www.annualcreditreport.com o llame sin cargo al 1-877-322-8228. Si no, complete un formulario de solicitud del informe de solvencia anual (que puede descargar en https://www.consumer.ftc.gov/articles/0155-free-credit-reports) y envíelo a la siguiente dirección para obtener un ejemplar: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Para los residentes de *Iowa*: Según la legislación estatal, se recomienda que informe cualquier sospecha que tenga de que se produjo un robo de la identidad ante los organismos de seguridad o la fiscalía general.

Para los residentes de *Oregón*: Según las leyes estatales, se recomienda que informe cualquier sospecha que tenga de que se produjo un robo de la identidad ante los organismos de seguridad, o incluso a la fiscalía general o a la Comisión Federal de Comercio.

Para los residentes de Maryland, Rhode Island, Illinois, Nueva York y Carolina del Norte: En las oficinas de la fiscalía general o de la Comisión Federal de Comercio de Maryland y de Carolina del Norte pueden brindarle información sobre las alertas por fraude, los bloqueos de seguridad y las medidas que puede tomar para evitar que se produzca un robo de la identidad.
Maryland Office of the Attorney General Consumer Protection Division (Protección al consumidor de la fiscalía general de Maryland), 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection (Protección al consumidor de la fiscalía general de Rhode Island), 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division (Protección al consumidor de la fiscalía general de Carolina del Norte), 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center (Centro de atención al consumidor de la Comisión Federal de Comercio), 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection (Área de fraude y protección al consumidor de la fiscalía general de Nueva York), The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Para los residentes de *Massachusetts*: Por la legislación estatal estamos obligados a informarle que tiene derecho a obtener un informe policial si sufrió el robo de su identidad.

Para los residentes de todos los estados:
Alertas por fraude: Puede poner alertas por fraude en las tres oficinas crediticias por teléfono y en línea. Ingrese a Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), TransUnion (https://www.transunion.com/fraud-alerts) o Experian (https://www.experian.com/fraud/center.html). Con las alertas por fraude se les dan a los acreedores ciertos procedimientos que deben seguir, como comunicarse con usted, antes de abrir cuentas nuevas o modificar las actuales. Por ese motivo, si bien poner una alerta lo puede proteger, también puede causar demoras si quiere obtener crédito. Desde el 21 de septiembre de 2018, las alertas por fraude que se disponen por primera vez se prolongan por un año, aunque las víctimas de robo de la identidad pueden extenderlas por siete años. En la parte inferior de esta página aparecen los números telefónicos de las tres agencias crediticias.

Monitoreo: Siempre debe estar alerta y revisar las cuentas por si se registra actividad sospechosa o inusual.

Bloqueo de seguridad: Además, tiene derecho a colocar un bloqueo de seguridad en su informe de solvencia. El bloqueo de seguridad está pensado para evitar que se aprueben créditos, préstamos o servicios a su nombre sin su autorización. Para ello, debe hacer el pedido ante cada agencia crediticia, el cual puede ser por correo postal certificado, correo exprés o estampillado postal; si no, puede seguir las instrucciones que aparecen en los sitios web que se indican a continuación. Cuando lo solicite debe incluir la siguiente información (tenga en cuenta que si lo pide para su cónyuge o para un menor de 16 años, también tendrá que suministrar los datos de esa persona): (1) nombre completo, con la inicial del segundo nombre y la fórmula de tratamiento; (2) el número de Seguro Social; (3) la fecha de nacimiento; (4) el domicilio actual y los de los últimos cinco años; y (5) la correspondiente denuncia o el informe del incidente que obtuvo del organismo de seguridad o del Registro Automotor. Además, debe incluir una copia de la tarjeta de identificación estatal y una factura de servicios, un estado de cuenta bancario o un extracto del seguro de emisión reciente. Es fundamental que todas las páginas sean legibles y que en ellas conste su nombre, la dirección postal actual y la fecha de emisión. Desde el 21 de septiembre de 2018, no se cobra por colocar, levantar ni quitar los bloqueos. Además, puede solicitarlos para los menores de 16 años. Si desea obtener un bloqueo de seguridad sin costo, comuníquese con una o más de las siguientes agencias crediticias del país:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

Puede comunicarse con la Comisión Federal de Comercio (Federal Trade Commission), cuyos datos aparecen en esta carta.

EXHIBIT B

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>
<<Address_1>> <<Address_2>>
<<City>>, <<State>> <<Zip Code>>

April 27, 2021

Dear <<First Name>> <<Last Name>>:

You are receiving this letter because we became aware on or about Tuesday February 9, 2021 that County files containing your personal information were recently released at a publicly accessible website maintained by the cyber threat actor(s) responsible for the October 2020 ransomware attack that affected Chatham County (hereinafter, the "Incident"). This letter contains information about the Incident, how the Incident may have impacted your personal information, steps we are taking to address the Incident, and actions you can take to safeguard your information.

What Happened

The County of Chatham experienced a ransomware attack in October 2020. During a typical ransomware attack, cybercriminals try to "lock" an organization's digital files in an attempt to get paid for a digital key to unlock the files. Sometimes, as was the case here, the cybercriminals will also acquire files from the organization they have targeted and post those files at a publicly accessible location on the internet, commonly referred to as the "dark web."

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to: your name, date of birth, home address, phone number, social security number and/or health information from your personnel file if you are a current or former Chatham County employee. If you have received any services from DSS including child welfare services this may have also included information maintained by DSS such as your name, the names of your household members, and employer and/or wages connected with DSS forms and notes.

What We Are Doing

The County's investigation of this incident remains ongoing and we are in close communication with our law enforcement partners on this issue. We have also worked closely with the North Carolina Emergency Management and a third-party information technology forensics firm to determine how the attack occurred in an effort to prevent it from happening again.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection 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, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 27, 2021.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. That said, we strongly encourage you to remain vigilant and monitor your account statements for any suspicious activity. We also recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

A call center has been established to assist you. If you have any additional questions, please do not hesitate to call 1-833-903-3648.

Sincerely,

Dan J. LaMontagne, PE
Chatham County Manager

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Para inscribirse, llame al:
1-833-903-3648
o visite:
https://app.idx.us/account-creation/protect
Código de inscripción:
<<XXXXXXXX>>

A/C IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<Nombre>> <<Segundo nombre>> <<Apellido>> <<Fórmula de tratamiento>>
<<Dirección_1>> <<Dirección_2>>
<<Ciudad>>, <<Estado>> <<Código postal>>

27 de abril de 2021

Estimado/a <<Nombre>> <<Apellido>>:

Le enviamos esta carta porque advertimos que el martes 9 de febrero de 2021, o cerca de esa fecha, se dieron a conocer en un sitio web accesible públicamente los archivos del condado en los que constaba su información personal. Dicho sitio corresponde al ejecutor/es de amenazas cibernéticas responsable/s del ataque de chantaje (*ransomware*) ocurrido en octubre de 2020, el cual afectó al condado de Chatham (en adelante, el «incidente»). En la presente carta se le brinda información sobre el incidente, cómo este puede haber repercutido en su información personal, los pasos que estamos tomando para corregirlo y las medidas que usted puede llevar adelante para proteger sus datos.

Qué ocurrió

El condado de Chatham sufrió un ataque de chantaje en octubre de 2020. Lo que ocurre en este tipo de circunstancias es que los cibercriminales tratan de «bloquear» los archivos digitales de determinada organización con el objetivo de que se les pague a cambio de una clave digital para desbloquearlos. Hay veces en que, como ocurrió en este caso, los cibercriminales obtienen archivos de la organización que atacaron y los publican en ciertos sitios de Internet con acceso público, lo que comúnmente se denomina «Internet profunda».

¿Qué información se vio afectada?

Posiblemente, entre los datos personales que se expusieron se encuentran los siguientes, aunque puede haber habido más: su nombre, fecha de nacimiento, domicilio, número de teléfono, número de Seguro Social y/o información médica que consta en su expediente personal si es o fue un empleado del condado de Chatham. Si recibió los servicios del Departamento de Servicios Sociales (DSS por sus siglas en inglés), como los de protección a menores, posiblemente la información que tenía dicho organismo en los formularios o notas también hayan quedado expuesta, como su nombre y los de las personas que viven con usted y su empleador o el sueldo.

Qué estamos haciendo

El condado sigue investigado lo ocurrido y está en estrecha comunicación con las fuerzas del orden público que colaboran con nosotros en referencia a este tema. Además, trabajamos codo a codo con la división de manejo de emergencias de Carolina del Norte y con una firma de informática forense para establecer cómo se produjo el ataque con el fin de evitar que vuelva a ocurrir.

Asimismo, le ofrecemos los servicios de protección contra el robo de la identidad de IDX, expertos en filtración y recuperación de datos, que contemplan lo siguiente: doce meses de monitoreo crediticio y con CyberScan, una póliza de reintegros de $1.000.000, así como servicios completos de recuperación ante el hurto de la identidad. Con la protección de IDX, se podrán solucionar problemas en caso de que su identidad se viese vulnerada.

Qué puede hacer usted

Le recomendamos que se comunique con IDX por cualquier pregunta que tenga y para inscribirse en los servicios gratuitos para la protección de la identidad. Llame al 1-833-903-3648 o ingrese a https://app.idx.us/account-creation/protect y utilice el código de inscripción que aparece al principio de esta carta. Los representantes de IDX lo atenderán de lunes a viernes de 9 a. m . a 9 p. m. hora del este. Tenga en cuenta que la inscripción cierra el 27 de julio de 2021.

No tenemos conocimiento de que alguien haya sido víctima de fraude como consecuencia del incidente hasta ahora. No obstante, le recomendamos fervientemente que esté alerta y revise los estados de cuenta bancarios para ver si hay actividad sospechosa. Además, le sugerimos que lea la siguiente página que contiene información importante sobre las medidas que usted puede tomar para proteger su información personal, tales como implementar alertas por fraude o bloqueos de seguridad.

Para obtener más información

Se dispuso un centro de atención para responder a sus consultas. Si tiene preguntas, no dude en llamar al 1-833-903-3648.

Atentamente,

Ing. Dan J. LaMontagne
Administrador del condado de Chatham

Más información importante

Para los residentes de *Hawái*, *Míchigan*, *Misuri*, *Virginia*, *Vermont* y *Carolina del Norte*: La legislación estatal recomienda que esté alerta ante casos de incidentes de fraude o robo de la identidad. Para ello, revise si en los extractos de las tarjetas de crédito o en los informes de solvencia se registra actividad no autorizada.

Para los residentes de *Illinois*, *Iowa*, *Maryland*, *Misuri*, *Carolina del Norte*, *Oregón* y *Virginia Occidental*:
Por la legislación estatal estamos obligados a informarle que puede obtener un ejemplar sin costo de su informe de solvencia, ya sea que sospeche que hubo actividad no autorizada en su cuenta o no. Puede obtener un ejemplar gratuito de cada una de las tres oficinas crediticias del país. Para solicitarlo, ingrese a www.annualcreditreport.com o llame sin cargo al 1-877-322-8228. Si no, complete un formulario de solicitud del informe de solvencia anual (que puede descargar en https://www.consumer.ftc.gov/articles/0155-free-credit-reports) y envíelo a la siguiente dirección para obtener un ejemplar: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Para los residentes de *Iowa*: Según la legislación estatal, se recomienda que informe cualquier sospecha que tenga de que se produjo un robo de la identidad ante los organismos de seguridad o la fiscalía general.

Para los residentes de *Oregón*: Según las leyes estatales, se recomienda que informe cualquier sospecha que tenga de que se produjo un robo de la identidad ante los organismos de seguridad, o incluso a la fiscalía general o a la Comisión Federal de Comercio.

Para los residentes de Maryland, Rhode Island, Illinois, Nueva York y Carolina del Norte: En las oficinas de la fiscalía general o de la Comisión Federal de Comercio de Maryland y de Carolina del Norte pueden brindarle información sobre las alertas por fraude, los bloqueos de seguridad y las medidas que puede tomar para evitar que se produzca un robo de la identidad.
Maryland Office of the Attorney General Consumer Protection Division (Protección al consumidor de la fiscalía general de Maryland), 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection (Protección al consumidor de la fiscalía general de Rhode Island), 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division (Protección al consumidor de la fiscalía general de Carolina del Norte), 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center (Centro de atención al consumidor de la Comisión Federal de Comercio), 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection (Área de fraude y protección al consumidor de la fiscalía general de Nueva York), The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Para los residentes de *Massachusetts*: Por la legislación estatal estamos obligados a informarle que tiene derecho a obtener un informe policial si sufrió el robo de su identidad.

Para los residentes de todos los estados:
Alertas por fraude: Puede poner alertas por fraude en las tres oficinas crediticias por teléfono y en línea. Ingrese a Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), TransUnion (https://www.transunion.com/fraud-alerts) o Experian (https://www.experian.com/fraud/center.html). Con las alertas por fraude se les dan a los acreedores ciertos procedimientos que deben seguir, como comunicarse con usted, antes de abrir cuentas nuevas o modificar las actuales. Por ese motivo, si bien poner una alerta lo puede proteger, también puede causar demoras si quiere obtener crédito. Desde el 21 de septiembre de 2018, las alertas por fraude que se disponen por primera vez se prolongan por un año, aunque las víctimas de robo de la identidad pueden extenderlas por siete años. En la parte inferior de esta página aparecen los números telefónicos de las tres agencias crediticias.

Monitoreo: Siempre debe estar alerta y revisar las cuentas por si se registra actividad sospechosa o inusual.

Bloqueo de seguridad: Además, tiene derecho a colocar un bloqueo de seguridad en su informe de solvencia. El bloqueo de seguridad está pensado para evitar que se aprueben créditos, préstamos o servicios a su nombre sin su autorización. Para ello, debe hacer el pedido ante cada agencia crediticia, el cual puede ser por correo postal certificado, correo exprés o estampillado postal; si no, puede seguir las instrucciones que aparecen en los sitios web que se indican a continuación. Cuando lo solicite debe incluir la siguiente información (tenga en cuenta que si lo pide para su cónyuge o para un menor de 16 años, también tendrá que suministrar los datos de esa persona): (1) nombre completo, con la inicial del segundo nombre y la fórmula de tratamiento; (2) el número de Seguro Social; (3) la fecha de nacimiento; (4) el domicilio actual y los de los últimos cinco años; y (5) la correspondiente denuncia o el informe del incidente que obtuvo del organismo de seguridad o del Registro Automotor. Además, debe incluir una copia de la tarjeta de identificación estatal y una factura de servicios, un estado de cuenta bancario o un extracto del seguro de emisión reciente. Es fundamental que todas las páginas sean legibles y que en ellas conste su nombre, la dirección postal actual y la fecha de emisión. Desde el 21 de septiembre de 2018, no se cobra por colocar, levantar ni quitar los bloqueos. Además, puede solicitarlos para los menores de 16 años. Si desea obtener un bloqueo de seguridad sin costo, comuníquese con una o más de las siguientes agencias crediticias del país:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

Puede comunicarse con la Comisión Federal de Comercio (Federal Trade Commission), cuyos datos aparecen en esta carta.