Aviso de incidente de seguridad de datos

La Liga Puertorriqueña Contra El Cáncer DBA Hospital Oncológico ("Hospital Oncológico") ha tomado conocimiento de un incidente de seguridad de datos que puede haber resultado en un acceso sin autorización de su información personal confidencial. Hospital Oncológico lamenta sinceramente cualquier inconveniente o preocupación que este asunto pueda causar y sigue dedicado a garantizar la privacidad y seguridad de toda la información bajo nuestro control.

¿Qué pasó? El día 17 de mayo del 2024, El Hospital Oncológico tuvo conocimiento de un posible compromiso de correo electrónico empresarial que involucraba la cuenta de correo electrónico de Microsoft 365 ("M365") de un empleado. Al descubrir el incidente, el Hospital Oncológico contrató de inmediato a una empresa especializada en ciberforense para realizar una investigación forense para determinar el alcance y circunstancias que resultaron en el incidente. Inicialmente, la investigación forense se completó el 17 de julio del 2024 y determinó que no hubo acceso no autorizado, ni afectado por la PHI. Sin embargo, tras una investigación adicional, se descubrieron registros adicionales para su análisis y la investigación forense se reabrió el 17 de julio del 2024. El 19 de julio del 2024, se completó la investigación forense sobre los registros adicionales y se confirmó que hubo un acceso no autorizado a la cuenta de correo electrónico del empleado. Actualmente, El Hospital Oncológico está analizando el contenido de la cuenta de correo electrónico en busca de cualquier posible información personal sensible ("PII") o información de salud protegida ("PHI"). El Hospital Oncológico está trabajando para identificar a todas las personas específicas y el tipo de datos a los que potencialmente se accedió con el fin de proporcionar suficiente aviso a las personas. El Hospital Oncológico enviará cartas de notificación formal a las personas afectadas una vez que sean identificadas.

¿De qué información se trataba? La investigación sigue en curso. Sin embargo, si se descubre que la información confidencial ha sido potencialmente comprometida, se enviará una carta de notificación formal a aquellos que hayan sido afectados, sobre su información confidencial, la carta identificará los tipos de información que fueron afectados.

Lo que estamos haciendo. El Hospital Oncológico se compromete a garantizar la privacidad y seguridad de toda la información personal bajo nuestro cuidado. Desde el descubrimiento del incidente, el Hospital Oncológico ha tomado y continuará tomando medidas para mitigar el riesgo de problemas futuros. En concreto, el Hospital Oncológico ha contratado a una empresa especializada en ciberseguridad para que realice una investigación forense para determinar la naturaleza y el alcance del incidente y ha cambiado las contraseñas y ha reforzado los requisitos de contraseñas. Además, se han implementado prácticas de seguridad adicionales que incluyen volver a capacitar a los empleados, actualizar las políticas e implementar un escaneo de seguridad semanal del sitio para determinar si hay algún problema.

Si hubo acceso no autorizado a al información confidencial, el Hospital Oncológico ofrecerá servicios complementarios de monitoreo de crédito y protección contra el robo de identidad a las personas afectadas. Se enviarán cartas de notificación a las personas afectadas con la información para inscribirse en los servicios de monitoreo de crédito. El Hospital Oncológico anima a todas las personas identificadas a inscribirse en este servicio gratuito.

Lo que puedes hacer. El Hospital Oncológico recomienda a todos los miembros a permanecer atentos a incidentes de robo de identidad y fraude, a revisar los estados de cuenta y a monitorear los informes de crédito para detectar actividades sospechosas o no autorizadas. Además, los expertos en seguridad sugieren que las personas se comuniquen con su institución financiera y con todas las principales agencias de crédito para informarles de dicha violación y tomar las medidas recomendadas para proteger sus intereses, incluida la posible colocación de una alerta de fraude en el archivo de crédito.

Para más información. El Hospital Oncológico reconoce que nuestros miembros pueden tener preguntas que no se abordan en este aviso. Los representantes están disponibles durante 90 días a partir de la fecha de esta publicación para ayudarlos con cualquier pregunta relacionada con este incidente, entre las 8:00 a. m. y las 8:00 p. m., hora del este, de lunes a viernes, excepto días festivos. Llame al 1-833-763-4149 con cualquier pregunta que tenga sobre este aviso.

Pasos que puede seguir para ayudar a proteger su información

Informes de crédito: Puede obtener una copia de su informe de crédito, de forma gratuita, ya sea que sospeche o de cualquier actividad no autorizada en su cuenta. Puede obtener una copia gratuita de su informe de crédito de cada una de las tres agencias de informes de crédito a nivel nacional. Para solicitar su informe de crédito gratuito, visite www.annualcreditreport.com o llame gratis al 1-877-322-8228. También puede solicitar su informe de crédito anual gratuito enviando por correo un Formulario de Solicitud de Informe de Crédito Anual completo (disponible en https://www.consumer.ftc.gov/articles/0155-free-credit-reports) a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Alertas de fraude: Puede colocar alertas de fraude con las tres agencias de crédito por teléfono o en línea. Una alerta de fraude les dice a los acreedores que sigan ciertos procedimientos, incluido el contacto con usted, antes de abrir nuevas cuentas o cambiar sus cuentas existentes. Por esa razón, colocar una alerta de fraude puede protegerlo, pero también puede retrasarlo cuando busque obtener crédito. A partir del 21 de septiembre del 2018, las alertas iniciales de fraude duran un año. Las víctimas de robo de identidad también pueden recibir una alerta de fraude extendida durante siete años.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 https://www.equifax.com/personal/credit-reportar-servicios/alertas-de-fraude-crediticio/

Monitoreo: Siempre debe permanecer atento a incidentes de fraude y robo de identidad revisando los estados de cuenta de las tarjetas de crédito y monitoreando su informe de crédito para detectar actividades sospechosas o inusuales.

Congelamiento de seguridad: Usted tiene derecho a colocar un congelamiento de seguridad en su informe de crédito. Un congelamiento de seguridad tiene como objetivo evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. Para colocar un congelamiento de seguridad en su informe de crédito, debe hacer una solicitud a cada agencia de informes del consumidor. Puede hacer esa solicitud por correo certificado, correo urgente, correo regular sellado o siguiendo las instrucciones que se encuentran en los sitios web que se enumeran a continuación. Se debe incluir la siguiente información al solicitar un congelamiento de seguridad (tenga en cuenta que si está solicitando un informe de crédito para su cónyuge o un menor de 16 años, esta información también debe proporcionarse para él/ella): (1) nombre completo, con la inicial del segundo nombre y cualquier sufijo; (2) Número de Seguro Social; (3) fecha de nacimiento; (4) dirección actual y cualquier dirección anterior de los últimos cinco años; y (5) cualquier informe o queja de incidente aplicable ante una agencia de aplicación de la ley o el Registro de Vehículos Motorizados. La solicitud también debe incluir una copia de una tarjeta de identificación emitida por el gobierno y una copia de una factura reciente de servicios públicos o un estado de cuenta bancaria o de seguro. Es esencial que cada copia sea legible, muestre su nombre y dirección postal actual, y la fecha de emisión. Al partir del 21 de septiembre del 2018, es gratis colocar, levantar o eliminar un congelamiento de seguridad. También puede colocar un congelamiento de seguridad para niños menores de 16 años. Puede obtener un congelamiento de seguridad gratuito comunicándose con una o más de las siguientes agencias nacionales de informes del consumidor:

Experian	**TransUnion**	**Equifax**
Apartado Postal 9554 Allen, TX 75013 1-888-397-3742	Apartado Postal 160 Woodlyn, PA 19094 1-888-909-8872	Apartado de correos 105788 Atlanta, GA 30348-5788 1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-servicios-de-informes/congelamiento-de-credito/

Presentar una denuncia policial: Usted tiene derecho a presentar o obtener una denuncia policial si sufre fraude de identidad. Tenga en cuenta que para presentar una denuncia de delito o una denuncia de incidente ante la policía por robo de identidad, es probable que deba proporcionar pruebas de que ha sido víctima. A menudo se requiere un informe policial para disputar artículos fraudulentos. Por lo general, puede denunciar incidentes sospechosos de robo de identidad a la policía local o al Fiscal General.

FTC y Procuradores Generales: Puede informarse más sobre el robo de identidad, las alertas de fraude, los congelamientos de seguridad y las medidas que puede tomar para protegerse, comunicándose con el informe del consumidor y la Comisión Federal de Comercio (FTC, por sus siglas en inglés) o el Procurador General de su estado. Puede comunicarse con la Comisión Federal de Comercio al: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. La Comisión Federal de Comercio (FTC, por sus siglas en inglés) también alienta a aquellos que descubran que su información ha sido utilizada indebidamente a presentar una queja ante ellos.

Para los residentes de *Iowa*: La ley estatal le aconseja denunciar cualquier sospecha de robo de identidad a la policía o al Fiscal General.

Para los residentes de *Massachusetts*: La ley estatal exige que se le informe de su derecho a obtener un informe policial presentado con respecto a este incidente. Si usted es víctima de robo de identidad, también tiene derecho a presentar una denuncia policial y obtener una copia de la misma.

Para los residentes de *Nuevo México*: La ley estatal le aconseja revisar los estados de cuenta personales y los informes de crédito, según corresponda, para detectar errores resultantes de la violación de seguridad. Usted tiene derechos de conformidad con la Ley de Informes de Crédito Justos, como el derecho a que se le informe si la información de su expediente crediticio se ha utilizado en su contra, el derecho a saber lo que hay en su expediente crediticio, el derecho a solicitar su puntaje crediticio y el derecho a disputar la información incompleta o inexacta. Además, de conformidad con la Ley de Informes de Crédito Justos, las agencias de informe del consumidor deben corregir o eliminar la información inexacta, incompleta o no verificable; Las agencias de informe del consumidor no pueden reportar información negativa obsoleta; El acceso a su archivo es limitado; debe dar su consentimiento para que se proporcionen informes de crédito a los empleadores; Usted puede limitar las ofertas "preseleccionadas" de crédito y seguro que recibe en función de la información de su informe de crédito; y puede reclamar daños y perjuicios a los infractores. Es posible que tenga derechos adicionales en virtud de la Ley de Informe de Crédito Justos que no se describen aquí. Las víctimas de robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos de conformidad con la Ley de Informes de Crédito Justos. Le recomendamos que revise sus derechos de conformidad con la Ley de Informes de Crédito Justos en www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf o escribiendo a Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Para los residentes de Oregon: La ley estatal le aconseja denunciar cualquier sospecha de robo de identidad a las fuerzas del orden, incluido el Fiscal General y la Comisión Federal de Comercio.

Para los residentes de Vermont: Si no tiene acceso a Internet pero desea obtener más información sobre cómo colocar un congelamiento de seguridad en su informe de crédito, comuníquese con la Oficina del Fiscal General de Vermont al 802-656-3183 (800-649-2424 línea gratuita solo en Vermont).

Para los residentes de Rhode Island: La ley estatal exige que se le informe de su derecho a presentar o obtener un informe policial con respecto a este incidente.

Para los residentes de *Arizona, Colorado, Distrito de Columbia, Illinois, Maryland, Nueva York, Carolina del Norte y Rhode Island:* Puede obtener información de las Oficinas del Procurador General y la Comisión Federal de Comercio sobre alertas de fraude, congelamientos de seguridad y medidas que puede tomar para prevenir el robo de identidad.

Comisión Federal de Comercio - Centro de Respuesta al Consumidor: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Sección de Defensa y Protección al Consumidor de la Oficina del Procurador General de Arizona: , 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Oficina del Procurador General de Colorado: Protección al Consumidor 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

Oficina del Procurador General del Distrito de Columbia: – Oficina de Protección al Consumidor: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Oficina del Procurador General de Illinois - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-9995630**;** www.illinoisattorneygeneral.gov

Oficina del Procurador General de Maryland: es posible que también desee revisar la información proporcionada por el Maryland Abogado Generalen cómo Para evitar identidad robo en https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, o enviando un correo electrónico a idtheft@oag.state.md.uso llamando al 410-576-6491.

Oficina del Procurador General de Nueva York : puede comunicarse y obtener información de estas agencias estatales: *División de Protección al Consumidor del Departamento de Estado de Nueva York*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; y *Oficina del Fiscal General del Estado de Nueva York,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

Oficina del Procurador General de Carolina del Norte: se puede contactar al Procurador General en el Centro de Servicios Postales 9001, Raleigh, NC 27699-9001, 1-877-566-7226 o 1-919-716-6400, y www.ncdoj.gov. También puede obtener información sobre los pasos que puede tomar para prevenir el robo de identidad. Fiscal General de Carolina del Norte en https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

Oficina del Procurador General de Rhode Island: Protección al Consumidor: 150 South Main St., Providence RI 02903**;** 1401-274-4400**;** www.riag.ri.gov.

Notice of Data Security Incident

La Liga Puertorriquena Contra El Cancer DBA Hospital Oncológico ("Hospital Oncológico') has become aware of a data security Incident that may have resulted in an unauthorized access to your sensitive personal information. Hospital Oncológico sincerely regrets any inconvenience or concern that this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

What Happened? On May 17, 2024, La Liga Puertorriquena Contra El Cancer DBA Hospital Oncológico ("Hospital Oncológico') became aware of a potential business email compromise involving the Microsoft 365 ("M365") email account of an employee. Upon discovering the Incident, Hospital Oncológico promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. Initially, the forensic investigation was completed on July 17, 2024 and determined that there was no PHI impacted or unauthorized access. However, upon further inquiry additional logs for analysis were discovered and the forensic investigation was reopened on July 17, 2024. On July 19, 2024, the forensic investigation into the additional logs was completed and confirmed there was an unauthorized access on the employee's email account. Hospital Oncológico is currently analyzing of the contents of the email account for any potential sensitive personal information ("PII") or protected health information ("PHI"). Hospital Oncológico is working to identify all the specific individuals and the type of data that was potentially accessed in order to provide sufficient notice to individuals. Hospital Oncológico will mail formal notice letters to those impacted individuals once they are identified.

What Information Was Involved? The investigation is still ongoing. However, if sensitive information is found to have been potentially compromised, a formal notice letter will be sent to those who have had their sensitive information impacted, and the letter will identify the types of information involved.

What We Are Doing. Hospital Oncológico is committed to ensuring the privacy and security of all personal information in our care. Since the discovery of the Incident, Hospital Oncológico has taken and will continue to take steps to mitigate the risk of future issues. Specifically, Hospital Oncológico has engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident and changed passwords and strengthened password requirements. Also, additional security practices have been implemented that include retraining employees, updating policies, and implementing a weekly security scan of the site to determine if there are any issues.

If there was unauthorized access to sensitive information, Hospital Oncológico will be offering complimentary credit monitoring and identity theft protection services to those impacted individuals. Notification letters will be sent to those impacted individuals with the information to enroll in the credit monitoring services. Hospital Oncológico encourages all identified individuals to register for this free service.

What You Can Do. Hospital Oncológico encourages all members to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that individuals contact his/her financial institution and all major credit bureaus to inform them of such a breach and take the recommended steps to protect his/her interests, including the possible placement of a fraud alert on the credit file.

For More Information. Hospital Oncológico recognizes that our members may have questions not addressed in this notice. Representatives are available for 90 days from the date of this posting to assist you with any questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call 1-833-763-4149 with any questions you have surrounding this notice.

Steps You Can Take to Help Protect Your Information

Credit Reports: 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.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You 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:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting

agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

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 *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. **Federal Trade Commission -** Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-9995630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - you may also may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

New York Office of Attorney General - you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Office of the Attorney General - the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;** 1401-274-4400**;** www.riag.ri.gov.