



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 11, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Service Employees International Union Local 32BJ (“32BJ”), located at 25 W. 18th Street, New York, New York 10011, and write to notify your office of an incident that may affect the security of some personal information relating to approximately thirteen thousand, four hundred thirty-eight (13,438) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, 32BJ does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 1, 2021, 32BJ experienced a data security incident that impacted a limited number of 32BJ computer systems. 32BJ immediately responded and launched an investigation with cybersecurity experts to confirm the nature and scope of the incident and determine the impact to 32BJ data. Through the investigation, 32BJ learned that an unauthorized actor accessed certain files and folders within the 32BJ system and may have viewed or acquired data containing certain employee and member information between October 21, 2021 until November 1, 2021.

32BJ conducted a thorough programmatic and manual review of the impacted files and folders to determine whether it contained any sensitive data. 32BJ recently concluded its review and determined on or around January 13, 2021 that information related to certain individuals was included in the impacted files. After determining the scope of information in the impacted files,

32BJ undertook efforts to locate address information for the affected individuals, put resources in place, and provide direct notice.

The information that could have been subject to unauthorized access includes name, address, Social Security number, financial account number, driver's license number, and passport number.

Notice to Maryland Residents

Beginning on February 11, 2022, 32BJ provided written notice of this incident to all affected individuals, which includes approximately thirteen thousand, four hundred thirty-eight (13,438) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, 32BJ moved quickly to investigate and respond to the incident, assess the security of 32BJ systems, and notify potentially affected individuals. 32BJ is also working to implement additional safeguards and training to its employees. 32BJ is providing access to credit monitoring services for 12 months, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, 32BJ is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. 32BJ is providing individuals with information on how to place a fraud alert and security freeze on one's credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4554.

Very truly yours,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/mzb
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

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

<<Date>>

NOTICE OF <<VARIABLE HEADER>>

Dear <<Name 1>>:

Service Employees International Union, Local 32BJ, (“32BJ”) writes to make you aware of a recent incident that may impact the privacy of some of your information. You are receiving this letter because you are potentially impacted by this incident. 32BJ is providing you with notice of the incident, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On November 1, 2021, 32BJ experienced a data security incident that impacted a limited number of 32BJ computer systems. We immediately responded and launched an investigation with cybersecurity experts to confirm the nature and scope of the incident and determine the impact to 32BJ data. Through the investigation, we learned that an unauthorized actor accessed certain files and folders within the 32BJ system and may have viewed or acquired data containing certain member information between October 21, 2021 until November 1, 2021.

We conducted a thorough programmatic and manual review of the potentially impacted files and folders to determine whether they contained any sensitive data. We recently concluded our review and determined on or around January 13, 2022, that information related to you was included in the potentially impacted files. After determining the scope of information in the impacted files, we undertook efforts to locate address information for the affected individuals, put resources in place, and provide this direct notice.

What Information Was Involved? The information present in the files that may have been viewed or acquired as a result of this incident included your name, and <<breached elements>>.

What We Are Doing. We treat our responsibility to safeguard the information entrusted to us as an utmost priority. As such, we responded immediately to this incident and have been working diligently to provide you with an accurate and complete notice of the incident. Our immediate response to this event also included prompt and continued correspondence with federal law enforcement authorities. As part of our ongoing commitment to the privacy and security of information in our care, we are reviewing our existing policies and procedures relating to data protection and security and implemented enhanced security controls on our remote access system. We also changed system passwords and upgraded our security tools. We will continue to evaluate additional security measures to mitigate any potential risk associated with this incident and to better prevent similar incidents in the future.

As an added precaution, we are providing you with <<12/24>> months of complimentary access to credit monitoring and identity restoration services through Equifax, as well as guidance on how to better protect your information. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter.

What You Can Do. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at 855-604-1832, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time excluding U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Torre', with a long horizontal stroke extending to the right.

David Torre
Director of Technology & Operations
Service Employees International Union, Local 32BJ

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring / Identity Protection

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Enrollment Instructions

Enter your Activation Code: <<ACTIVATION CODE>>

Enrollment Deadline: <<ENROLLMENT DEADLINE>>

Go to www.equifax.com/activate and enter your unique Activation Code of <<Activation Code>> then click “Submit” and follow these 4 steps:

1. **Register:** Complete the form with your contact information and click “Continue”. If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click ‘Sign Me Up’ to finish enrolling. The confirmation page shows your completed enrollment. Click “View My Product” to access the product features.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report.
- Daily access to your Equifax credit report.
- WebScan notifications when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites.
- Automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock.
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf.
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft (conditions apply).

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. SEIU 32BJ is located at 25 W. 18th Street New York, New York 10011.

For New Mexico residents, 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 bureaus 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 violator. 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 by visiting 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 1,169 Rhode Island residents impacted by this incident.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Date>>

NOTIFICACIÓN SOBRE <<SPANISH HEADER>>

Estimado(a) <<Name 1>>:

La Local 32BJ de la Unión Internacional de Empleados de Servicios (32BJ) le escribe para alertarle sobre un reciente incidente que podría impactar la privacidad de una parte de su información. Usted está recibiendo esta carta porque es probable que usted haya sido impactado por dicho incidente. La 32BJ le está ofreciendo la notificación del incidente, los pasos que hemos tomado en respuesta a eso, y los recursos a su disposición para ayudarle a proteger mejor su información, si usted considera que es apropiado hacerlo.

¿Qué sucedió? El 1º de noviembre de 2021, la 32BJ experimentó un incidente de seguridad de datos que impactó a un número limitado de sistemas de computación de la 32BJ. Nosotros respondimos de inmediato y lanzamos una investigación con expertos de ciberseguridad para confirmar la naturaleza y el alcance del incidente y determinar el impacto que tuvo en los datos de la 32BJ. Gracias a la investigación, hallamos que un agente no autorizado logró acceder a ciertos documentos y carpetas dentro del sistema de la 32BJ y podría haber visto o adquirido datos conteniendo cierta información sobre nuestros miembros entre el 21 de octubre de 2021 y el 1º de noviembre de 2021.

Nosotros realizamos una revisión programática exhaustiva y manual de los archivos y carpetas potencialmente impactados para determinar si éstos contenían algún tipo de información delicada. Concluimos nuestro análisis recientemente y, alrededor del 13 de enero, determinamos que información sobre usted fue parte de los archivos potencialmente impactados. Tras determinar el alcance de la información de los archivos impactados, nosotros tomamos medidas para localizar la información de domicilios de las personas afectadas, asignar los recursos apropiados y brindar esta notificación directa.

¿Qué tipo de información fue afectada? La información contenida en los archivos que podrían haber sido vistos o adquiridos como resultado de este incidente incluyó su nombre y <<breached elements>>.

¿Qué estamos haciendo? Nosotros consideramos la responsabilidad de proteger la información confiada a nosotros como de alta prioridad. Como tal, nosotros respondimos de inmediato a este incidente y hemos trabajado diligentemente para proporcionarle a usted una notificación precisa y exhaustiva del incidente. Nuestra respuesta inmediata ante este evento incluyó correspondencia continua e inmediata con las autoridades federales del orden. Como parte de nuestro compromiso continuo con la privacidad y seguridad de la información a nuestro cargo, estamos revisando nuestras políticas y procedimientos existentes respecto a la protección y seguridad de los datos; e implementamos controles de seguridad adicionales a nuestro sistema de acceso remoto. Asimismo, cambiamos las contraseñas del sistema y actualizamos nuestras herramientas de seguridad. Seguiremos evaluando medidas de seguridad adicionales para atenuar todo riesgo potencial asociado con este incidente y para prevenir incidentes similares en el futuro.

Como precaución adicional, le estamos brindando a usted <<12/24>> meses de acceso de cortesía para monitorear su crédito y usar servicios de restauración de identidad mediante Equifax, así como pautas de cómo proteger mejor su información personal. Pese a que nosotros cubriremos los costos de estos servicios, y dadas las restricciones de privacidad, será necesario que usted mismo complete el proceso de activación usando las instrucciones de inscripción adjuntas a esta carta.

¿Qué puede usted hacer? Usted puede averiguar más sobre cómo proteger su información en el documento adjunto: *Pasos que puede usted dar para proteger su información personal*. Allí, usted hallará información adicional sobre el monitoreo de crédito y los servicios de restauración de identidad que estamos le ofrecemos de cortesía y de cómo inscribirse.

Para mayor información. Entendemos que usted podría tener preguntas sobre este incidente que no se han abordado en esta carta. Para asegurarnos de que sus preguntas son respondidas de manera oportuna, sírvase llamar a nuestra línea exclusiva de asistencia al 855-604-1832, de lunes a viernes de 9:00 am a 9:00 pm hora del este. Eastern Time, excluyendo los festivos oficiales de los E.E.U.U.

Sinceramente,

David Torre
Director de Tecnología y Operaciones
Local 32BJ, Unión Internacional de Empleados de Servicios

PASOS QUE PUEDE USTED DAR PARA PROTEGER SU INFORMACIÓN PERSONAL

Inscríbase en el monitoreo de crédito/protección de identidad

Instrucciones para inscripción

Acceda a www.equifax.com/activate e ingrese su código de activación único de <<Activation Code>>, luego haga clic en “Submit” (Enviar) y siga estos 4 pasos:

1. **Registro:** Complete el formulario con su información de contacto y haga clic en “Continue” (Continuar). Si usted ya tiene una cuenta myEquifax, haga clic en el enlace “Sign in here” (Iniciar sesión aquí) en el encabezado “Let’s get started” (Comencemos). Una vez que haya iniciado sesión correctamente, pasará a la página de pago en el Paso 4.
2. **Creación de una cuenta:** Ingrese su dirección de correo electrónico, cree una contraseña y acepte los términos de uso.
3. **Verificación de identidad:** Para inscribirse en su producto, le pediremos que complete nuestro proceso de verificación de identidad.
4. **Pago:** Tras la verificación exitosa de su identidad, verá la página de pago. Haga clic en “Sign Me Up” (Registrarme) para finalizar la inscripción. La página de confirmación muestra su inscripción completada. Haga clic en “View My Product” (Ver mi producto) para acceder a las funciones del producto.

Características clave

- Monitoreo de crédito con notificaciones por correo electrónico acerca de cambios clave en su informe de crédito de Equifax
- Acceso diario a su informe de crédito de Equifax
- Notificaciones de WebScan: cuando su información personal, como su número de Seguro Social, números de tarjeta de crédito/débito o de cuenta bancaria se encuentran en sitios fraudulentos de transacciones por Internet
- Alertas automáticas de fraude, que alerta a los posibles prestamistas a tomar medidas adicionales para verificar su identidad antes de extender créditos, además de alertas de consulta bloqueadas y bloqueo de informe de crédito de Equifax
- Restauración de identidad para ayudar a restaurar su identidad en caso de que sea víctima de robo de identidad, y un especialista en restauración de identidad dedicado para trabajar en su nombre
- Hasta \$1,000,000 de cobertura de seguro contra robo de identidad para ciertos gastos de bolsillo que resulten del robo de identidad (se aplican condiciones)

Monitorear sus cuentas

Bajo la ley de E.E.U.U., usted tiene derecho a un reporte de crédito anual de cortesía de cada una de las principales agencias de reporte de crédito. Para solicitar su reporte de crédito de cortesía, visite www.annualcreditreport.com o llame, libre de cargo, al 1-877-322-8228. Usted también puede contactar a las tres principales agencias de crédito para solicitar una copia gratuita de su reporte de crédito.

Los consumidores tienen derecho a solicitar que se coloque una “alerta por fraude” inicial o prolongada en un archivo personal de crédito, sin costo alguno. Una alerta inicial por fraude es una alerta de un (1) año que se coloca en el archivo de crédito de un consumidor. Al ver que existe una alerta por fraude en el archivo de crédito de un consumidor, todo negocio está obligado a dar pasos para verificar la identidad del consumidor antes de otorgar una nueva línea de crédito. Si es usted víctima de robo de identidad, usted tiene derecho a una alerta prolongada de fraude, que es una alerta de fraude que dura siete años. Si usted desea colocar una alerta de fraude, sírvase contactar a cualquiera de las tres principales agencias de reportes de crédito listadas más adelante.

Como alternativa a una alerta por fraude, los consumidores tienen derecho a solicitar un “congelamiento de crédito” en un archivo personal de crédito, lo que le prohibiría a la agencia de crédito revelar información contenido en el archivo de crédito sin la expresa autorización del consumidor. El congelamiento de crédito está diseñado para prevenir que se aprueben créditos, préstamos y servicios a nombre suyo sin su consentimiento. Sin embargo, usted debe ser consciente que al usar un congelamiento de crédito para controlar quién podría tener acceso a la información personal y financiera en su reporte de crédito, podría dilatar, interferir o prohibir la aprobación oportuna de cualquier pedido o solicitud subsecuente que usted mismo haga por un nuevo préstamo, crédito, hipoteca o cualquier otro tipo de cuenta que involucre una extensión de crédito. En conformidad con la ley federal, a usted no se le puede cobrar por ya sea colocar o suspender un congelamiento de crédito en su reporte de crédito. Para solicitar un congelamiento de crédito, usted deberá proporcionar la siguiente información:

1. Nombre completo (incluyendo su inicial media, así como los sufijos Jr., Sr., II, III, etc.);
2. Número de seguridad social;
3. Fecha de nacimiento;
4. Domicilios durante los cinco años anteriores;
5. Prueba de su actual domicilio, tales como un recibo de luz o de teléfono;
6. Una fotocopia legible de alguna tarjeta de identificación emitida por el gobierno (licencia de conducir o tarjeta de identidad estatal, etc.); y
7. Una copia del reporte policial, reporte investigativo o queja ante una agencia del orden respecto al robo de identidad si usted fue víctima de robo de identidad.

Si usted desea solicitar un congelamiento de crédito, sírvase contactar a las tres principales agencias de reporte de crédito listadas a continuación:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Información adicional

Usted podrá instruirse más respecto al robo de identidad, alerta por fraude, congelamiento de crédito y los pasos que usted puede tomar para proteger su información personal, contactando a las agencias de reporte de consumidores, la Comisión Federal de Comercio, o al Procurador General de su estado. A la Comisión Federal de Comercio la puede contactar en: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. La Comisión Federal de Comercio le recomienda a toda persona que descubra que han abusado de su información, a que presenten una queja ante ellos. Usted puede obtener mayor información sobre cómo presentar una de esas quejas usando la información arriba. Usted tiene derecho a presentar un reporte policial si usted ha sido víctima de robo de identidad o fraude. Sírvase notar que para presentar una queja por robo de identidad ante una agencia de la ley, usted probablemente deberá proporcionar prueba de que usted ha sido víctima de esto. Casos de robo de identidad conocidos o sospechados también deben presentarse ante las agencias del orden y el Procurador General de su estado. Esta notificación no ha sido dilatada por las agencias del orden.

Para residentes del Distrito de Columbia, el Procurador General para el Distrito de Columbia puede ser contactado en: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

Para residentes de Maryland, el Procurador General de Maryland puede ser contactado en: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; y www.oag.state.md.us. 32BJ SEIU está ubicada en el 25 W. 18th Street, New York, New York 10011.

Para residentes de Nuevo México, en conformidad con el Acta de Reportes Justos de Crédito, usted tiene derechos tales como el derecho a que se le informe si la información en su archivo de crédito ha sido usada en su contra, el derecho a saber qué hay en su reporte de crédito, el derecho a solicitar su nivel de crédito y el derecho a cuestionar toda información incompleta o incorrecta. Más aún, en conformidad con el Acta de Reportes Justos de Crédito, las agencias de reporte de consumidores deben corregir o borrar información incorrecta, incompleta o no verificable; las agencias de reportes de consumidores no podrán revelar información negativa caduca; el acceso a su archivo está limitado; usted deberá dar su consentimiento para que reportes de crédito le puedan ser proporcionados a cualquier empleador; usted puede asimismo limitar las ofertas “pre-aprobadas” de crédito y seguros que usted reciba que se basen en su reporte de crédito; y usted puede pedir compensación por daños a quienes viole esto. Usted podría tener más derechos según el Acta de Reportes Justos de Crédito no incluidas aquí. Las víctimas de robo de identidad y el personal de servicio militar activo tienen derechos específicos según el Acta de Reportes Justos de Crédito. Le recomendamos revisar sus derechos en conformidad con el Acta de Reportes Justos de Crédito visitan www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; o si les escribe al Consumer Center Response, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Para residentes de Nueva York, el Procurador General de Nueva York puede ser contactado en: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; o visite <https://ag.ny.gov/>.

Para residentes de Carolina del Norte, el Procurador General de Carolina del Norte se le pueden encontrar en: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 o al 1-919-716-6000; y www.ncdoj.gov.

Para residentes de Rhode Island, el Procurador General de Rhode Island puede ser contactado en: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Bajo las leyes de Rhode Island, usted tiene derecho a obtener cualquier reporte policial presentado en conexión con este incidente. Hay 1,169 residentes de Rhode Island impactados por este incidente.