

Notice of Data Incident

The Hertz Corporation, on behalf of Hertz, Dollar and Thrifty brands (collectively, “Hertz,” “we,” or “us”), is providing notice of an event involving Cleo Communications US, LLC (“Cleo”), a vendor of Hertz, that may have impacted the personal information of certain individuals. This notice provides details about the event, measures we have taken in response, and additional steps potentially impacted individuals can take to help protect their personal information, if they feel it is necessary to do so.

Cleo is a vendor that provides a file transfer platform used by Hertz for limited purposes. On February 10, 2025, we confirmed that Hertz data was acquired by an unauthorized third party that we understand exploited zero-day vulnerabilities within Cleo’s platform in October 2024 and December 2024. Hertz immediately began analyzing the data to determine the scope of the event and to identify individuals whose personal information may have been impacted.

We completed this data analysis on April 2, 2025, and concluded that the personal information involved in this event may include the following: name, contact information, date of birth, credit card information, driver’s license information and information related to workers’ compensation claims. A very small number of individuals may have had their Social Security or other government identification numbers, passport information, Medicare or Medicaid ID (associated with workers’ compensation claims), or injury-related information associated with vehicle accident claims impacted by the event.

Hertz takes the privacy and security of personal information seriously. To that end, Hertz has confirmed that Cleo took steps to investigate the event and address the identified vulnerabilities. Hertz also reported this event to law enforcement and is in the process of reporting the event to relevant regulators. Further, out of an abundance of caution, Hertz has secured the services of Kroll to provide two years of identity monitoring or dark web monitoring services to potentially impacted individuals at no cost. Potentially impacted residents of the United States may sign up for identity monitoring services here: <http://hufcuwxgqzil.kroll.com/>.

While Hertz is not aware of any misuse of personal information for fraudulent purposes in connection with the event, we encourage potentially impacted individuals, as a best practice, to remain vigilant to the possibility of fraud or errors by reviewing account statements and monitoring free credit reports for any unauthorized activity and reporting any such activity. We have also included additional resources below.

We understand that there may be questions about this event that are not addressed in this notice. For additional information, please call **(866) 408-8964** Monday through Friday, from 6:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays.

Additional Resources:

Individuals should remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, an individual may be entitled every 12 months to one free copy of the individual’s credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. Consumers may wish to stagger their requests so that they receive free reports from one of the three credit bureaus every four months.

A consumer can place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on an individual’s credit file. Upon seeing a fraud alert displayed on an individual’s credit file, a business must verify the individual’s identity before extending new credit. Victims of identity theft may be entitled to an extended fraud alert, which is a fraud alert lasting seven years. To place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, an individual has the right to place a “credit freeze” (also referred to as a “security freeze”) on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the individual’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in the individual’s name without the individual’s consent. However, please be aware that using a credit freeze to control who can access an individual’s personal and financial information in the individual’s credit report may delay, interfere with, or prohibit

the timely approval of any subsequent request or application the individual makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, an individual cannot be charged to place or lift a credit freeze on the individual's credit report. The following information will need to be provided to request a credit freeze: (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 the individual is a victim of identity theft.

To place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below.

Equifax: Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069; Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788; <https://www.equifax.com/personal/credit-report-services/>; 1-888-298-0045

Experian: Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013; Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013; <https://www.experian.com/help/>; 1-888-397-3742

TransUnion: TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016; TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094; <https://www.transunion.com/credit-help>; 1-800-916-8800

Individuals may educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect personal information by contacting the individual reporting bureaus (as described above), the Federal Trade Commission, or their state Attorney General. In particular, the Federal Trade Commission encourages those who discover their information has been misused to file a complaint. Individuals can obtain further information on filing such a complaint by using the contact information listed below.

An individual can file a police report in the event of identity theft or fraud. Please note that, to file a report with law enforcement for identity theft, an individual will likely need to provide some proof of the identity theft. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General.

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

Maryland Residents: Individuals may contact and obtain information from Maryland Attorney General 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.

Massachusetts Residents: Individuals can file a police report in the event of identity theft or fraud. Under Massachusetts law, an individual may have the right to file and obtain a copy of a police report. Individuals may also have the right to request a security freeze, as described above. Individuals may contact and obtain information from the Massachusetts Attorney General at One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. Instances of known or suspected identity theft should also be reported to law enforcement and the Attorney General.

New Mexico Residents: Individuals have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit files, the right to ask for their credit scores, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the individual reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to individuals' files is limited; individuals must give consent for credit reports to be provided to employers; individuals may limit "prescreened" offers of credit and insurance based on information in credit reports; and individuals may seek damages from violators. Individuals 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. For more information about rights available under the Fair Credit Reporting Act, visit 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.

New York Residents: Individuals may contact and obtain information from the New York Office of the Attorney General at The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

North Carolina Residents: Individuals may contact and obtain information from the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

Rhode Island Residents: Individuals may contact and obtain information from the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event.

Washington, D.C. Residents: Individuals may have the right to request a security freeze, as described above. Individuals may contact and obtain information from the Office of the Attorney General for the District of Columbia at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

Aviso de Incidente de Datos

The Hertz Corporation, en nombre de las marcas Hertz, Dollar y Thrifty (colectivamente, "Hertz", "nosotros" o "nos"), está brindando el aviso de un evento que involucra a Cleo Communications US, LLC ("Cleo"), un proveedor de Hertz, que puede haber afectado la información personal de ciertas personas. Este aviso proporciona detalles sobre el evento, las medidas que hemos tomado en respuesta y los pasos adicionales que las personas potencialmente afectadas pueden tomar para proteger su información personal, si consideran que es necesario hacerlo.

Cleo es un proveedor que ofrece una plataforma de transferencia de archivos que Hertz utiliza para fines limitados. El 10 de febrero de 2025, confirmamos que los datos de Hertz fueron adquiridos por un tercero no autorizado que entendemos efectuó ataques de vulnerabilidad de día cero en la plataforma de Cleo en octubre de 2024 y diciembre de 2024. De inmediato, Hertz comenzó a analizar los datos para determinar el alcance del evento e identificar a las personas cuya información personal pudo haberse visto afectada.

Completamos este análisis de datos el 2 de abril de 2025 y concluimos que la información personal involucrada en este evento puede incluir lo siguiente: nombre, información de contacto, fecha de nacimiento, información de la tarjeta de pago, información de la licencia de conducir e información relacionada con reclamos de compensación laboral. Es posible que el evento haya afectado a un número muy pequeño de personas en relación a su número de Seguro Social u otros números de identificación gubernamental, información de pasaporte, identificación de Medicare o Medicaid (asociada con reclamos de compensación laboral), o información relacionada con lesiones asociada con reclamos de accidentes vehiculares afectados por el evento.

Hertz se toma en serio la privacidad y la seguridad de la información personal. Con ese fin, Hertz ha confirmado que Cleo tomó medidas para investigar el evento y abordar las vulnerabilidades identificadas. Hertz también informó este evento a la policía y está en proceso de informarlo a los reguladores pertinentes. Además, por precaución, Hertz ha contratado los servicios de Kroll para brindar dos años de monitoreo de identidad o monitoreo de la dark web a las personas potencialmente afectadas sin costo alguno. Los residentes de los Estados Unidos potencialmente afectados pueden inscribirse en los servicios de monitoreo de identidad aquí: <http://hufcuwxgqzil.kroll.com/>.

Si bien Hertz no tiene conocimiento de ningún uso indebido de información personal con fines fraudulentos en relación con el evento, alentamos a las personas potencialmente afectadas, como mejor práctica, a permanecer atentas a la posibilidad de fraude o errores revisando los estados de cuenta y monitoreando los informes de crédito gratuitos para detectar cualquier actividad no autorizada y denunciar dicha actividad. También hemos incluido recursos adicionales a continuación. Entendemos que puede haber preguntas sobre este evento que no se abordan en este aviso. Para obtener información adicional, llame a **(866) 408-8964**, de lunes a viernes, de 6:00 a. m. a 8:00 p. m., hora central, excepto los principales días festivos de EE. UU.

Recursos adicionales:

Las personas deben mantenerse alertas revisando los estados de cuenta y monitoreando los informes de crédito. Según la ley federal, también tiene derecho cada 12 meses a una copia gratuita de su informe de crédito de cada una de las tres principales compañías de informes crediticios. Para obtener un informe de crédito anual gratuito, vaya a www.annualcreditreport.com o llame al 1-877-322-8228. Es posible que los usuarios deseen escalar sus solicitudes para recibir informes gratuitos de una de las tres agencias de crédito cada cuatro meses.

Un usuario puede colocar una "alerta de fraude" inicial o extendida en un expediente crediticio sin costo alguno. Una alerta de fraude inicial es una alerta de un año que se coloca en el expediente crediticio de una persona. Al ver una alerta de fraude en el expediente crediticio de una persona, una empresa debe verificar la identidad de esa persona antes de otorgarle un nuevo crédito. Es posible que las víctimas de robo de identidad tengan derecho a una alerta de fraude extendida, que es una alerta de fraude que dura siete años. Para colocar una alerta de fraude, comuníquese con cualquiera de las tres principales agencias de informes crediticios que se mencionan a continuación.

Como alternativa a una alerta de fraude, una persona tiene derecho a colocar un "bloqueo de crédito" (también conocido como "bloqueo de seguridad") en un informe de crédito, lo que prohibirá a una agencia de crédito divulgar información en el informe crediticio sin la autorización expresa de la persona. El bloqueo crediticio está diseñado para evitar que se aprueben créditos, préstamos y servicios a nombre de una persona sin su consentimiento. Sin embargo, tenga en cuenta que el uso de un bloqueo

de crédito para controlar quién puede acceder a la información personal y financiera de una persona en su informe crediticio puede demorar, interferir o prohibir la aprobación oportuna de cualquier solicitud o pedido posterior que haga con respecto a un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta que involucre la extensión del crédito. De conformidad con la ley federal, no se puede cobrar a una persona por colocar o retirar un bloqueo crediticio en su informe crediticio. Se deberá proporcionar la siguiente información para solicitar un bloqueo de crédito: (1) Nombre completo (incluida la inicial del segundo nombre, así como Jr., Sr., II, III, etc.); (2) Número de Seguro Social; (3) Fecha de nacimiento; (4) Direcciones de los últimos dos a cinco años; (5) Evidencia de dirección actual, como un recibo de servicios públicos o un recibo telefónico actual; (6) Una fotocopia legible de un documento de identidad emitido por el gobierno (licencia de conducir estatal o documento de identidad, etc.); y (7) Una copia del informe policial, informe de investigación o denuncia puesta en una agencia policial sobre robo de identidad si la persona es víctima de robo de identidad.

Para colocar una alerta de fraude o bloqueo de crédito, comuníquese con las tres principales oficinas de informes crediticios que se mencionan a continuación.

Equifax: Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069; Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788; <https://www.equifax.com/personal/credit-report-services/>; 1-888-298-0045

Experian: Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013; Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013; <https://www.experian.com/help/>; 1-888-397-3742

TransUnion: TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016; TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094; <https://www.transunion.com/credit-help>; 1-800-916-8800

Los usuarios pueden obtener más información sobre el robo de identidad, las alertas de fraude, los bloqueos crediticios y los pasos que pueden seguir para proteger su información personal si se comunican con las agencias encargadas de suministrar informes crediticios, la Comisión Federal de Comercio (Federal Trade Commission) de los Estados Unidos o el fiscal general de su estado. En particular, la Comisión Federal de Comercio anima a quienes descubran que su información ha sido utilizada indebidamente para presentar una denuncia. Las personas pueden obtener más información sobre cómo presentar una queja de este tipo utilizando la información de contacto que aparece a continuación.

Una persona puede presentar una denuncia ante la policía en caso de robo de identidad o fraude. Tenga en cuenta que, para presentar un informe ante las autoridades policiales por robo de identidad, es probable que la persona deba proporcionar alguna evidencia del robo de identidad. Los casos de robo de identidad, sean confirmados o presuntos, también se deben informar ante las autoridades policiales y el fiscal general del estado correspondiente.

Todos los residentes de los EE. UU.: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261.

Residentes de Maryland: las personas pueden comunicarse y obtener información del Fiscal General de Maryland en 200 St. Paul Place, piso 16, Baltimore, MD 21202; 1-410-528-8662 o 1-888-743-0023; y en www.oag.state.md.us.

Residentes de Massachusetts: las personas pueden presentar una denuncia ante la policía en caso de robo de identidad o fraude. Según la ley de Massachusetts, una persona puede tener derecho a presentar y obtener una copia de un informe policial. Como se indicó anteriormente, las personas también tienen derecho a solicitar el bloqueo de seguridad. Las personas pueden comunicarse y obtener información del Fiscal General de Massachusetts en One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. Los casos de robo de identidad, sean confirmados o presuntos, también se deben informar ante las autoridades policiales y el fiscal general.

Residentes de Nuevo México: las personas tienen derechos de conformidad con la Ley de Informes de Crédito Justos (Fair Credit Reporting Act), como por ejemplo, el derecho a ser informadas si la información en su expediente crediticio se ha utilizado en su contra, el derecho a conocer lo que está en su expediente crediticio, el derecho a solicitar su puntaje crediticio, y el derecho a impugnar información incompleta o inexacta. Asimismo, de conformidad con la Ley de Informes de Crédito Justos, las oficinas de preparación de los informes de las personas deben corregir o eliminar la información inexacta, incompleta o no verificable; las agencias de preparación de los informes de los usuarios no pueden comunicar información negativa desactualizada; el acceso a los expedientes de las personas está limitado; las personas deben prestar su consentimiento para que los informes crediticios se envíen a los empleadores; las personas pueden limitar las ofertas de crédito y seguro "preseleccionadas" basado en la información contenida en sus informes crediticios y las personas pueden demandar a los infractores por daños y perjuicios. Es posible que en virtud de la Ley de Informes de Crédito Justos tenga derechos adicionales que no se han resumido aquí. Las víctimas de robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos en virtud de la Ley Federal de Informe Imparcial de Crédito. Para mayor información sobre los derechos

disponibles según la Ley de Informes de Crédito Justos, visite el sitio web www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o escriba al Centro de Respuestas al Consumidor en: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Residentes de Nueva York: las personas pueden comunicarse y obtener información de la Oficina del Fiscal General de Nueva York en The Capitol, Albany, NY 12224-0341; 1-800-771-7755; o en <https://ag.ny.gov/>.

Residentes de Carolina del Norte: las personas pueden comunicarse y obtener información del Fiscal General de Carolina del Norte en 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 o 1-919-716-6000; y en www.ncdoj.gov.

Residentes de Rhode Island: las personas pueden comunicarse y obtener información del Fiscal General de Rhode Island en 150 South Main Street, Providence, RI 02903; 1-401-274-4400; y en www.riag.ri.gov. Conforme a la legislación de Rhode Island, las personas tienen derecho a obtener una copia de toda denuncia policial presentada en relación con este incidente.

Residentes de Washington, DC: las personas pueden tener derecho a solicitar un bloqueo de seguridad, como se describe anteriormente. Las personas pueden comunicarse y obtener información de la Oficina del Fiscal General del Distrito de Columbia en 400 6th Street, NW, Washington, DC 20001; 202-727-3400; y en oag@dc.gov.

Avis d'incident de Données

La société Hertz, au nom des marques Hertz, Dollar et Thrifty (collectivement, "Hertz" ou "nous"), transmet un avis d'événement impliquant Cleo Communications US, LLC ("Cleo"), un fournisseur de Hertz, susceptible d'avoir eu un impact sur les informations personnelles de certaines personnes. Cet avis fournit des précisions sur l'événement, les mesures que nous avons prises en réponse à cet incident et les mesures supplémentaires que les personnes susceptibles d'être concernées peuvent prendre pour aider à protéger leurs informations personnelles, si elles jugent que cela est nécessaire.

Cleo est un fournisseur qui propose une plateforme de transfert de fichiers utilisée par Hertz à des fins limitées. Le 10 février 2025, nous avons pu confirmer que les données de Hertz ont été acquises par un tiers non autorisé qui, selon nous, a exploité les vulnérabilités zero-day de la plateforme Cleo en octobre et décembre 2024. Hertz a immédiatement commencé à analyser les données, afin de déterminer l'ampleur de l'événement et d'identifier les personnes dont les informations personnelles pourraient avoir été affectées.

Nous avons achevé cette analyse de données le 2 avril 2025 et il en résulte que les informations personnelles impliquées dans cet événement peuvent comprendre les informations suivantes : nom, coordonnées, date de naissance, informations de carte bancaire, informations sur le permis de conduire et informations relatives aux demandes d'indemnisation des employés. Un très petit nombre de personnes peuvent avoir eu leur numéro de sécurité sociale ou d'autres numéros d'identification officiels, des informations sur leur passeport, leur identifiant Medicare ou Medicaid (associé aux demandes d'indemnisation des employés), ou des informations relatives aux blessures associées aux réclamations d'accidents de véhicules affectées par l'événement.

Pour Hertz, la protection des informations personnelles est une priorité absolue. À cette fin, Hertz a indiqué que Cleo a mené une enquête sur l'événement et traité les failles détectées. Hertz a également signalé cet événement à la police et en a informé les autorités de régulation compétentes. De plus, par mesure de précaution, Hertz a fait appel à Kroll pour offrir gratuitement pendant deux ans des services de surveillance d'identitovigilance et du dark Web aux personnes susceptibles d'être concernées. Les résidents des États-Unis susceptibles d'être concernés peuvent s'inscrire aux services d'identitovigilance ici : <http://hufcuwxgqzil.kroll.com/>.

Bien que Hertz n'ait connaissance d'aucune utilisation frauduleuse des informations personnelles liée à cet incident, comme bonne pratique, nous encourageons les personnes potentiellement concernées à rester vigilantes quant aux possibilités de fraudes ou d'erreurs, en surveillant leurs relevés de compte et en vérifiant régulièrement leurs dossiers de crédit gratuits pour détecter toute activité non autorisée, et à signaler immédiatement toute anomalie. Nous avons également inclus des ressources supplémentaires ci-dessous.

Nous ne doutons pas que vous pouvez avoir des questions sur cet événement qui ne sont pas abordées dans cet avis. Pour obtenir des informations supplémentaires, veuillez appeler le **(866) 408-8964**, du lundi au vendredi, de 6 h 00 à 18 h 00 heure du Centre, sauf les principaux jours fériés aux États-Unis.

Ressources supplémentaires :

Les personnes concernées doivent rester vigilantes en examinant leurs relevés de compte et en surveillant leurs dossiers de crédit. Conformément à la loi fédérale, chaque personne a le droit d'obtenir gratuitement, une fois tous les 12 mois, un exemplaire de son rapport de crédit auprès de chacune des trois principales agences d'évaluation du crédit. Pour obtenir un dossier de crédit annuel gratuit, rendez-vous sur www.annualcreditreport.com ou appelez le 1-877-322-8228. Les consommateurs peuvent souhaiter échelonner leurs demandes, afin de recevoir des dossiers gratuits de l'une des trois agences de crédit tous les quatre mois.

Un consommateur peut une « alerte de fraude » initiale ou prolongée sur son dossier de crédit gratuitement. Une alerte de fraude initiale est une alerte d'un an activée dans le dossier de crédit d'une personne. Lorsqu'une alerte de fraude s'affiche dans le dossier de crédit de la personne, une entreprise doit vérifier l'identité de cette dernière avant d'accorder un nouveau crédit. Les victimes d'usurpation d'identité peuvent avoir droit à une alerte de fraude prolongée d'une durée de sept ans. Pour activer une alerte de fraude, veuillez contacter l'une des trois principales agences d'évaluation du crédit répertoriées ci-dessous.

À la place d'une alerte fraude, une personne peuvent opter pour un « blocage de crédit » (ou « gel de sécurité ») dans un dossier de crédit, qui interdit aux agences de crédit toute divulgation de leur rapport de crédit sans consentement écrit. Le gel de crédit vise à empêcher que des crédits, prêts et services soient accordés au nom d'une personne sans son

consentement. Cependant, veuillez noter qu'un gel de crédit, en limitant l'accès à vos informations personnelles et financières dans votre dossier de crédit, peut retarder, gêner ou empêcher l'acceptation rapide de toute future demande de prêt, crédit, hypothèque ou service impliquant l'octroi d'un crédit. Conformément à la législation fédérale, aucuns frais ne peuvent être appliqués pour la mise en place ou la levée d'un gel de crédit dans un dossier de crédit. Les informations suivantes doivent être fournies pour demander un gel de crédit : (1) Nom complet (y compris l'initiale du deuxième prénom, ainsi que Jr., Sr., II, III, etc.) ; (2) Numéro de sécurité sociale ; (3) Date de naissance ; (4) Adresses des deux à cinq dernières années ; (5) Justificatif de domicile, comme une facture d'électricité ou de téléphone ; (6) Une photocopie lisible d'une carte d'identité émise par le gouvernement (permis de conduire de l'État ou carte d'identité, etc.) ; et (7) Une copie du rapport de police, du rapport d'enquête ou de la plainte déposée auprès d'une autorité chargée de l'application de la loi concernant le vol d'identité si la personne est victime d'un vol d'identité.

Pour activer une alerte de fraude ou un gel de crédit, veuillez contacter les trois principales agences d'évaluation du crédit énumérées ci-dessous.

Equifax: Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 ; Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788 ; <https://www.equifax.com/personal/credit-report-services/> ; 1-888-298-0045

Experian: Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 ; Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013 ; <https://www.experian.com/help/> ; 1-888-397-3742

TransUnion: TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 ; TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094 ; <https://www.transunion.com/credit-help> ; 1-800-916-8800

Les personnes peuvent se renseigner sur le vol d'identité, les alertes à la fraude, les gels de crédit et les mesures qu'elles peuvent prendre pour protéger leurs informations personnelles en contactant les agences d'évaluation (aux coordonnées indiquées ci-dessus), la Federal Trade Commission ou le procureur général de leur État. En particulier, la Federal Trade Commission encourage les personnes découvrant une utilisation frauduleuse de leurs données à déposer plainte. Ces personnes peuvent obtenir de plus amples renseignements sur la manière de déposer une plainte en utilisant les coordonnées indiquées ci-dessous.

Une personne peut déposer une plainte auprès de la police en cas de vol d'identité ou de fraude. Veuillez noter que pour déposer une plainte auprès des services de police pour vol d'identité, la personne doit fournir une preuve du vol d'identité. Les cas de vol d'identité connus ou suspectés doivent être également signalés à la police et au procureur général de l'État concerné.

Tous les résidents des États-Unis : Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY : 1-866-653-4261.

Résidents du Maryland : Les personnes peuvent obtenir des informations supplémentaires auprès du procureur général du Maryland : 200 St. Paul Place, 16th Floor, Baltimore, MD 21202 ; 1-410-528-8662 ou 1-888-743-0023 ; et www.oag.state.md.us.

Résidents du Massachusetts : Les personnes peuvent déposer plainte auprès de la police en cas de vol d'identité ou de fraude. Conformément à la législation du Massachusetts, une personne peut avoir le droit de déposer plainte et obtenir une copie du rapport de police. Les personnes peuvent également avoir le droit de demander un gel de sécurité, comme décrit ci-dessus. Les personnes peuvent obtenir des informations supplémentaires auprès du procureur général du Massachusetts : One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. Les cas de vol d'identité connus ou suspectés doivent être également signalés à la police et au procureur général.

Résidents du Nouveau-Mexique : Conformément au Fair Credit Reporting Act, les personnes disposent de droits fondamentaux, notamment, du droit d'être informé si des informations contenues dans leur dossier de crédit ont été utilisées à leur encontre, du droit d'accès à l'intégralité de leur historique de crédit, du droit d'obtenir leur évaluation de crédit et du droit de contester des informations incomplètes ou inexacts. En outre, en vertu du Fair Credit Reporting Act, les agences d'évaluation doivent corriger ou supprimer les informations inexacts, incomplètes ou invérifiables ; les agences d'évaluation du crédit ne peuvent pas signaler les informations négatives et obsolètes ; l'accès aux dossiers des personnes est limité ; les personnes doivent donner leur consentement pour que les rapports de solvabilité soient fournis aux employeurs ; les personnes peuvent limiter les offres de crédit et d'assurance « présélectionnées » en fonction des informations contenues dans les dossiers de solvabilité ; et les victimes de violations de ces règles peuvent demander réparation devant les tribunaux. Les personnes peuvent avoir des droits supplémentaires en vertu du Fair Credit Reporting Act, qui ne sont pas résumés ici. Les victimes de vol d'identité et le personnel militaire en service actif disposent de droits

supplémentaires spécifiques en vertu du Fair Credit Reporting Act. Pour plus d'informations sur les droits disponibles en vertu du Fair Credit Reporting Act, rendez-vous sur www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf ou envoyez un courrier à Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Résidents de New York : Les personnes peuvent obtenir des informations supplémentaires auprès de procureur général de New-York : The Capitol, Albany, NY 12224-0341 ; 1-800-771-7755 ; ou <https://ag.ny.gov/>.

Résidents de la Caroline du Nord : Les personnes peuvent obtenir des informations supplémentaires auprès du procureur général de la Caroline du Nord : 9001 Mail Service Center, Raleigh, NC 27699-9001 ; 1-877-566-7226 ou 1-919-716-6000 ; et www.ncdoj.gov.

Résidents de Rhode Island : Les personnes peuvent obtenir des informations supplémentaires auprès du procureur général de Rhode Island : 150 South Main Street, Providence, RI 02903 ; 1-401-274-4400 ; et www.riag.ri.gov. En vertu de la législation de Rhode Island, les personnes ont le droit d'obtenir tout rapport de police déposé concernant cet événement.

Résidents de Washington, DC : Les personnes peuvent avoir le droit de demander le gel de sécurité, comme décrit ci-dessus. Les personnes peuvent obtenir des informations supplémentaires auprès du bureau du procureur général du district de Columbia : 400 6th Street, NW, Washington, DC 20001 ; 202-727-3400 ; et oag@dc.gov.