

EXHIBIT 1

This notice supplements the initial notice submitted to your Office on behalf of Sarku Japan on March 16, 2022. This notice will be further supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Sarku Japan does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about February 6, 2022, Sarku Japan discovered that an unauthorized actor gained access to certain Sarku Japan systems, and that information contained in those systems may have been viewed or taken by the unauthorized actor.

Sarku Japan reviewed the information in the systems to identify individuals with personal information that was potentially accessible during the event. Sarku Japan completed this review on February 10, 2022 and provided written notice of this incident to affected individuals on March 16, 2022, including one hundred thirty-one (131) Maine.

Subsequent review of additional information contained within the systems recently identified additional individuals whose information was potentially impacted by the incident, including two (2) additional Maine residents. The information that could have been subject to unauthorized access for these additional individuals includes the following: name, address, date of birth, and Social Security number.

Notice to Maine Residents

On or about August 8, 2022, Sarku Japan mailed notice to the additional two (2) Maine residents identified by Sarku Japan's subsequent review. 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, Sarku Japan moved quickly to investigate and respond to the incident, assess the security of Sarku Japan's systems, and notify potentially affected individuals. Sarku Japan is also working to implement additional safeguards and training to its employees. Sarku Japan is providing access to credit monitoring services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Sarku Japan 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. Sarku Japan is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF SECURITY INCIDENT

Dear <<First_Name>> <<Last_Name>>,

<<b2b_text_1(Variable State Holding Company)>> d/b/a Sarku Japan (“Sarku Japan”) is writing to inform you of an event that may impact the security of some of your information. This notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On February 6, 2022, Sarku Japan discovered anomalous activity within its computer network. Sarku Japan immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between January 14, 2022, and February 6, 2022, an unauthorized actor gained access to certain Sarku Japan systems and that information contained within those systems may have been viewed or taken by the unauthorized actor. Therefore, we conducted a thorough and in-depth review of the information within those systems to identify individuals with personal information that was potentially accessible. On June 1, 2022, we finalized this review to confirm the nature and scope of impacted data and the individuals to whom that data related. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, address, date of birth, and Social Security number may have been accessible.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to help protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are also offering identity monitoring services through Kroll for twelve (12) months, at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take To Help Protect Personal Information*. You may activate the complimentary identity monitoring services available to you. Activation instructions are attached to this letter.

For More Information. If you have additional questions, please call the dedicated assistance line at [1-XXX-XXX-XXXX](tel:1-XXX-XXX-XXXX), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready, which can be found in the enclosed *Attachment*.

Sincerely,

Tony Chiu
VP Finance & CFO
Sarku Japan

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

ACTIVATE IDENTITY MONITORING

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<Membership(S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES



You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 fraud alert or 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 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. SAR Holdings Inc. d/b/a Sarku Japan is located at 30 Broad Street, 14th Floor, New York, NY 10004.

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 thirteen \(13\) Rhode Island residents impacted by this incident.](#)



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

AVISO DE INCIDENTE DE SEGURIDAD

Estimado <<First_Name>> <<Last_Name>>,

<<b2b_text_1(Variable State Holding Company)>> d/b/a Sarku Japan (“Sarku Japan”) le escribe para informarle de un hecho que puede afectar a la seguridad de algunos de sus datos. Este aviso proporciona información sobre el evento, nuestra respuesta y los recursos disponibles para ayudarle a proteger su información de un posible uso indebido, si cree que es necesario hacerlo.

¿Qué ha pasado? El 6 de febrero de 2022, Sarku Japan descubrió una actividad anómala en su red informática. Sarku Japan abrió inmediatamente una investigación, con la ayuda de especialistas en ciberseguridad de terceros, para determinar la naturaleza y el alcance del evento. La investigación determinó que, entre el 14 de enero de 2022 y el 6 de febrero de 2022, un actor no autorizado obtuvo acceso a ciertos sistemas Sarku Japan y que la información contenida en esos sistemas puede haber sido vista o tomada por el actor no autorizado. Por lo tanto, realizamos una revisión exhaustiva y en profundidad de la información dentro de esos sistemas para identificar a las personas con información personal que fue potencialmente accesible. El 1 de junio de 2022, finalizamos esta revisión para confirmar la naturaleza y el alcance de los datos afectados y las personas con las que se relacionaron esos datos. Aunque no tenemos conocimiento de ningún uso indebido o intentado de su información personal, le proporcionamos este aviso por precaución.

¿Qué información estaba involucrada? La investigación determinó que su nombre, dirección, fecha de nacimiento y número de la Seguridad Social pueden haber sido accesibles.

Qué estamos haciendo. La confidencialidad, la privacidad y la seguridad de la información a nuestro cuidado son algunas de nuestras mayores prioridades. Al descubrir el problema, nos movimos rápidamente para investigar y responder a él, evaluar la seguridad de nuestros sistemas y notificar a las personas potencialmente afectadas. Estamos notificando a las personas potencialmente afectadas, incluido/a usted, para que pueda tomar más medidas para ayudar a proteger su información, si cree que es necesario hacerlo. Lamentamos cualquier inconveniente o preocupación que este problema pueda causar. Como precaución adicional, también ofrecemos servicios de monitoreo de identidad a través de Kroll durante doce (12) meses, sin costo para usted.

Qué puede hacer. Le recomendamos que permanezca alerta ante incidentes de robo de identidad y fraude mediante la revisión de sus estados de cuenta y los informes de crédito para detectar actividades sospechosas y que informe de cualquier actividad sospechosa de inmediato a su banco o institución financiera. Se incluyen información y recursos adicionales en los *Pasos que puede tomar para ayudar a proteger la información personal*. Puede activar los servicios gratuitos de monitoreo de identidad que tiene a su disposición. Las instrucciones de activación se adjuntan a esta carta.

Para obtener más información. Si tiene más preguntas, llame a la línea de asistencia dedicada al [1-XXX-XXX-XXXX](tel:1-XXX-XXX-XXXX), de lunes a viernes de 8:00 a. m. a 5:30 p. m., hora central, excluyendo los principales días festivos de los EE. UU. Por favor, tenga su número de socio listo, que se puede encontrar en el adjunto *incluido*.

Atentamente,

Tony Chiu
Vicepresidente de Finanzas y director financiero
Sarku Japan

PASOS QUE PUEDE SEGUIR PARA AYUDAR A PROTEGER LA INFORMACIÓN PERSONAL

ACTIVAR EL MONITOREO DE IDENTIDAD

Para ayudar a aliviar las preocupaciones y restaurar la confianza después de este incidente, hemos conseguido los servicios de Kroll para proporcionarle monitoreo de identidad sin costo durante un año. Kroll es un líder mundial en mitigación y respuesta al riesgo, y su equipo tiene una amplia experiencia ayudando a personas que han sufrido una exposición involuntaria de datos confidenciales. Sus servicios de monitoreo de identidad incluyen monitoreo de crédito, consulta de fraude y restauración de robo de identidad.

Visite <https://enroll.krollmonitoring.com> para activar y aprovechar sus servicios de monitoreo de identidad.

Tiene hasta el 4 de noviembre de 2022 para activar sus servicios de monitoreo de identidad.

Número de socio: <<Membership(S_N)>>

Para obtener más información sobre Kroll y sus servicios de monitorización de identidad, puede visitar info.krollmonitoring.com. Esta carta incluye información adicional que describe sus servicios.

APROVECHE SUS SERVICIOS DE MONITORIZACIÓN DE IDENTIDAD



Se le ha proporcionado acceso a los siguientes servicios de Kroll:

monitoreo de crédito de oficina única

Recibirá alertas cuando haya cambios en sus datos de crédito, por ejemplo, cuando se solicite una nueva línea de crédito en su nombre. Si no reconoce la actividad, tendrá la opción de llamar a un especialista en fraude de Kroll, que podrá ayudarle a determinar si es un indicador de robo de identidad.

Consulta sobre fraude

Tiene acceso ilimitado a una consulta con un especialista en fraude de Kroll. La asistencia incluye mostrarle las formas más efectivas de proteger su identidad, explicar sus derechos y protecciones de conformidad con la ley, asistencia con alertas de fraude e interpretar cómo se accede y usa la información personal, incluida la investigación de actividades sospechosas que podrían estar relacionadas con un evento de robo de identidad.

Restauración de robo de identidad

Si es víctima de robo de identidad, un investigador con licencia de Kroll con experiencia trabajará en su nombre para resolver problemas relacionados. Tendrá acceso a un investigador dedicado que entienda sus problemas y pueda hacer la mayor parte del trabajo por usted. Su investigador podrá profundizar para descubrir el alcance del robo de identidad y luego trabajar para resolverlo.

El sitio web de activación de Kroll solo es compatible con la versión actual o una versión anterior de Chrome, Firefox, Safari y Edge.

Para recibir servicios de crédito, debe ser mayor de 18 años y tener un crédito establecido en los EE. UU., tener un número de la Seguridad Social a su nombre y tener un domicilio en los EE. UU. asociado con su archivo de crédito.

MONITOREE SUS CUENTAS

Bajo la ley de los Estados Unidos, un consumidor tiene derecho a un informe de crédito gratuito anualmente de cada una de las tres principales agencias de informes de crédito, Equifax, Experian y TransUnion. Para solicitar su informe de crédito gratuito, visite www.annualcreditreport.com o llame sin cargo al 1-877-322-8228. También puede comunicarse directamente con las tres oficinas principales de informes de crédito que se enumeran a continuación para solicitar una copia gratuita de su informe de crédito.

Los consumidores tienen derecho a colocar una “alerta de fraude” inicial o extendida en un archivo de crédito sin costo alguno. Una alerta de fraude inicial es un aviso de 1 año que se coloca en el archivo de crédito de un consumidor. Al ver una alerta de fraude en el archivo de crédito de un consumidor, se requiere que una empresa tome medidas para verificar la identidad del consumidor antes de extender un nuevo crédito. Si es víctima de robo de identidad, tiene derecho a una alerta de fraude extendida, que es una alerta de fraude que dura siete años. Si desea colocar una alerta de fraude, comuníquese con cualquiera de las tres oficinas de informes de crédito principales que se enumeran a continuación.

Como alternativa a una alerta de fraude, los consumidores tienen el derecho a realizar una “congelación de crédito” en un informe crediticio, lo cual prohibirá a una oficina de crédito que divulgue información del informe crediticio sin la autorización expresa del consumidor. La congelación de crédito está diseñada para evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. No obstante, debería ser consciente de que utilizar una congelación de crédito para tener el control de quién accede a la información personal y financiera de su informe de crédito podría retrasar, interferir o impedir la aprobación a tiempo de cualquier solicitud o petición posterior que realice acerca de un nuevo préstamo, crédito, hipoteca o cualquier otro movimiento relacionado con una ampliación de crédito. Según la ley federal, no se le puede cobrar nada por realizar o levantar una congelación de crédito en su informe crediticio. Para solicitar una congelación de crédito, deberá proporcionar la siguiente información:

1. Nombre completo (incluyendo la inicial del medio, así como Jr., Sr., II, III, etc.);
2. Número de la Seguridad Social;
3. Fecha de nacimiento;
4. Direcciones en las que haya vivido durante los dos a cinco años anteriores;
5. Comprobante de la dirección actual, como una factura de servicios públicos actual o una factura telefónica;
6. Una fotocopia legible de un documento de identidad emitido por el gobierno (permiso de conducir o carnet de identidad, etc.); y
7. Una copia del informe policial, el informe de investigación o la queja a una agencia de la ley sobre el robo de identidad si es usted víctima de robo de identidad.

En caso de que desee realizar una alerta de fraude o una congelación de crédito, por favor, póngase en contacto con las tres grandes oficinas de informes crediticios que se enumeran 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

Puede informarse acerca del robo de identidad, alertas de fraude, congelaciones de crédito y los pasos que puede dar para proteger su información personal poniéndose en contacto con las oficinas de informes del consumidor, la Comisión Federal de Comercio o el fiscal general de su estado. Puede ponerse en contacto con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también anima a quienes descubran que se ha utilizado su información incorrectamente a que interpongan una queja ante ella. Puede obtener más información acerca de cómo presentar dicha queja en la información de contacto expuesta arriba. Tiene derecho a presentar una denuncia ante la policía si sufre alguna vez fraude o robo de identidad. Por favor, tenga en cuenta que para denunciar un robo de identidad ante la policía tendrá que proporcionar alguna prueba de que ha sido víctima de ello. Además, los casos de robo de identidad conocida o presunta deben denunciarse ante los cuerpos policiales y el fiscal general de su estado. Este aviso no ha sido retrasado por la aplicación de la ley.

Los residentes de Maryland pueden contactar con el fiscal general de Maryland en: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 o 1-888-743-0023; y www.oag.state.md.us. SAR Holdings Inc. d/b/a Sarku Japan se encuentra en 30 Broad Street, 14th Floor, New York, NY 10004.

Los residentes en Nuevo México tienen los derechos incluidos en la Ley de Informe Justo de Crédito (Fair Credit Reporting Act, FCRA), como el derecho a que le comuniquen si se ha utilizado contra usted la información de su informe crediticio, el derecho a saber qué incluye su informe crediticio, el derecho a preguntar su puntuación crediticia y el derecho a disputar la información incompleta o inexacta. Además, de conformidad con la Ley de Informe Justo de Crédito, las oficinas de informes de consumidores deben corregir o eliminar información inexacta, incompleta o no verificable; las agencias de informes de consumidores no pueden dar información negativa obsoleta; el acceso a su archivo es limitado; debe dar su consentimiento para que se proporcionen informes de crédito a los empleadores; puede limitar las ofertas “preseleccionadas” de crédito y seguro que obtiene en función de la información en su informe de crédito; y puede solicitar daños al infractor. Usted podría tener derechos adicionales según la Ley de Informe Justo de Crédito que no se encuentran resumidos aquí. Las víctimas de robos de identidad y el personal militar en servicio activo tienen derechos adicionales específicos bajo la Ley de Informe Justo de Crédito. Le animamos a revisar sus derechos otorgados por la Ley de Informe Justo de Crédito visitando www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o escribiendo al Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Los residentes de Nueva York pueden contactar con el fiscal general de Nueva York en: Oficina del fiscal general, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; o <https://ag.ny.gov/>.

Los residentes en Carolina del Norte pueden ponerse en contacto con el 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 www.ncdoj.gov.

Los residentes en Rhode Island pueden contactar con el fiscal general de Rhode Island en: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; y 1-401-274-4400. De conformidad con la ley de Rhode Island, usted tiene derecho a obtener cualquier denuncia policial presentada con relación a este incidente. [Hay trece \(13\) residentes de Rhode Island afectados por este incidente.](#)



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF SECURITY INCIDENT

Dear <<First_Name>> <<Last_Name>>,

<<b2b_text_1(Variable State Holding Company)>> d/b/a Sarku Japan (“Sarku Japan”) is writing to inform you of an event that may impact the security of some of your information. This notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On February 6, 2022, Sarku Japan discovered anomalous activity within its computer network. Sarku Japan immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between January 14, 2022, and February 6, 2022, an unauthorized actor gained access to certain Sarku Japan systems and that information contained within those systems may have been viewed or taken by the unauthorized actor. Therefore, we conducted a thorough and in-depth review of the information within those systems to identify individuals with personal information that was potentially accessible. On June 1, 2022, we finalized this review to confirm the nature and scope of impacted data and the individuals to whom that data related. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, address, date of birth, and Social Security number may have been accessible.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to help protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are also offering identity monitoring services through Kroll for twelve (12) months, at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take To Help Protect Personal Information*. You may activate the complimentary identity monitoring services available to you. Activation instructions are attached to this letter.

For More Information. If you have additional questions, please call the dedicated assistance line at [1-XXX-XXX-XXXX](tel:1-XXX-XXX-XXXX), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready, which can be found in the enclosed *Attachment*.

Sincerely,

Tony Chiu
VP Finance & CFO
Sarku Japan

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

ACTIVATE IDENTITY MONITORING

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<Membership(S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES



You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 fraud alert or 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 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. SAR Holdings Inc. d/b/a Sarku Japan is located at 30 Broad Street, 14th Floor, New York, NY 10004.

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 thirteen \(13\) Rhode Island residents impacted by this incident.](#)



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

安全事故通知

尊敬的 <<First_Name>> <<Last_Name>>，

<<b2b_text_1(Variable State Holding Company)>> d/b/a Sarku Japan (“Sarku Japan”)

写信通知您可能会影响您的某些信息安全的事件。本声明将提供有关该事件的信息、我们的反应以及如果您认为有必要，可用的帮助保护您的信息免遭可能的滥用的资源。

发生了什么事？2022年2月6日，Sarku Japan在其计算机网络中发现了异常活动。Sarku Japan在第三方网络安全专家的协助下，立即展开调查，以确定该事件的性质和范围。调查确定，在2022年1月14日至2022年2月6日期间，未经授权的人员获得了访问某些Sarku Japan系统的权限，并且这些系统中包含的信息可能已被未经授权的人员查看或获取了。因此，我们对这些系统内的信息进行了彻底和深入的审查，以识别具有潜在可访问的个人信息的个人。2022年6月1日，我们完成了本次审核，以确认受影响数据的性质和范围以及与该数据相关的个人。虽然我们不知道有任何实际或企图滥用您的个人信息的情况，但我们出于谨慎，向您提供此通知。

涉及哪些信息？调查确定，您的姓名、地址、出生日期和社会保障号码可能已经可以被获取。

我们采取的行动。我们所维护的信息的机密性、隐私性和安全性是我们最优先考虑的事项之一。得知该事件后，我们迅速采取行动，对事件进行调查和回应，评估我们系统的安全性，并通知可能受到影响的个人。我们会通知潜在受影响的个人（包括您），以便如果您认为有必要，您可以采取进一步措施来帮助保护您的信息。我们对此事件可能造成的不便或担忧深表歉意。作为额外的预防措施，我们还提供通过Kroll带来的身份监控服务，为期十二（12）个月，您无需支付任何费用。

您可以做什么。我们建议您通过查看您的帐户对账单和信用报告，随时警惕身份盗窃和欺诈事件，并及时向您的银行或金融机构报告任何可疑活动。随附的您可以采取哪些步骤来帮助保护个人信息中包含了其他信息和资源。您可以激活可用的免费身份监控服务。本函附有激活说明。

欲了解更多信息。如果您还有其他问题，请致电专用帮助热线 [1-XXX-XXX-XXXX](tel:1-XXX-XXX-XXXX)，工作时间为星期一至星期五上午8:00至下午5:30（美国中部时间，主要节假日除外）。请准备好您的会员号码，可以在随附的附件中找到。

此致，

Tony Chiu
财务副总裁兼首席财务官
Sarku Japan

您可以采取哪些步骤来帮助保护个人信息激活身份监控

为了帮助缓解此次事件带来的顾虑并恢复信任，我们已获得Kroll的服务，在一年内免费为您提供身份监控。Kroll是风险缓解和应对领域的全球领导者，他们的团队拥有丰富的经验，帮助那些无意被暴露机密数据的人。您的身份监控服务包括信用监控、欺诈咨询和身份盗窃恢复。

访问 <https://enroll.krollmonitoring.com> 激活并利用您的身份监控服务。您必须在2022年11月4日之前激活您的身份监控服务。

会员号：<<Membership(S_N)>>

欲知有关Kroll和您的身份监控服务的更多信息，您可以访问 info.krollmonitoring.com。本函附有描述您服务的其他信息。

使用您的身份监控服务

KROLL

您已获得Kroll提供的以下服务：

单局信用监控

当您的信用数据发生变化时（例如，当以您的名义申请新的信用额度时），您将收到提醒。如果您不能识别该活动，您可以选择致电Kroll欺诈专家，该专家将帮助您确定是否发生身份盗窃。

欺诈咨询

您可以无限制地向Kroll欺诈专家进行咨询。您所获得的专家支持包括向您展示保护身份的最有效方式，对于您的合法权利和可获得的法律保护做出解释，协助提供欺诈警报，解释如何获取和使用个人信息，包括调查可能与身份盗窃事件有关的可疑活动。

身份盗窃恢复

如果您成为身份盗窃的受害者，经验丰富的Kroll认证调查员将代表您解决相关问题。您可对接一位专门调查员，这位调查员了解您的问题，可以为您完成大部分工作。您的调查员将能够深入调查身份盗窃的范围，然后努力解决问题。

Kroll的激活网站仅与Chrome、Firefox、Safari和Edge的当前版本或前一版本兼容。

如需获得信用服务，您必须年满18岁，在美国已建立信用记录，名下拥有社会安全号码，并有与您的信用文件相关联的美国居住地址，并有与您的信用文件相关联的美国居住地址。

监控您的账户

根据美国法律，消费者有权每年从Equifax、Experian和TransUnion这三个主要信用报告机构中获取一份免费信用报告。如需获取免费信用报告，请访问 www.annualcreditreport.com或致电免费电话1-877-322-8228。您也可以直接联系下列的三家主要信用报告机构索取一份免费的信用报告。

消费者有权在信用档案中免费设置初始或延长时限的“欺诈警报”。初始欺诈警报是在消费者信用档案中设置的一年警报。当看到消费者信用档案上显示欺诈警报时，企业需要在产生新的信贷之前采取措施验证消费者的身份。如果您是身份盗窃的受害者，您有权获得延长的欺诈警报，即持续七年的欺诈警报。如果您希望设置欺诈警报，请联系以下三家主要信用报告机构中的任何一家。

作为欺诈警报的替代方案，消费者有权在信用报告上进行“信用冻结”，这将禁止信用机构在未经消费者明确授权的情况下发布信用报告中的信息。信用冻结的目的是防止未经您的同意以您的名义批准信贷、贷款和服务。尽管如此，您应知晓，使用信用冻结来控制他人访问您信用报告中的个人和财务信息，可能会延迟、干扰或禁止及时批准您就新贷款、信贷、抵押或任何其他涉及信用扩展的账户提出的任何后续请求或申请。根据联邦法律，在您的信用报告中设置或取消信用冻结不收取费用。如需申请信用冻结，您需要提供以下信息：

1. 全名（包括中间首字母，以及Jr、Sr、II、III等）；
2. 社会安全号码；
3. 出生日期；
4. 两年到五年间的地址；
5. 当前地址证明，如当前公用事业账单或电话账单；
6. 政府颁发的身份证（州驾照或身份证等）的清晰影印件；以及
7. 如果您是身份盗窃的受害者，请提供警方报告、调查报告或向执法机构投诉身份盗窃的副本。

如果您希望设置欺诈警报或信用冻结，请联系以下三家主要信用报告机构：

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

其他信息

您可以通过联系消费者报告机构、联邦贸易委员会或您所在州的总检察长，进一步了解身份盗窃、欺诈警报、安全冻结以及您可以采取哪些措施来保护自己。联邦贸易委员会的联系地址为：600 Pennsylvania Avenue NW, Washington, DC 20580；网址：www.identitytheft.gov；电话：1-877-身份盗窃专线（1-877-438-4338）；电传：1-866-653-4261。联邦贸易委员会还鼓励那些发现自己的信息被滥用的个人向他们提出投诉。您可以通过上面列出的联系方式获得有关如何提交此类投诉的更多信息。如果您曾遭遇身份盗窃或欺诈，您有权向警方报案。请注意，如需向执法部门提交身份盗窃报告，您可能需要提供一些证据证明您是受害者。已知或疑似身份盗窃的情况也应报告给执法部门和州检察长。本通知执法部门已经受理。

对于马里兰州居民，马里兰州总检察长的联系地址为：200 St. Paul Place, 16th Floor, Baltimore, MD 21202；电话：1-410-528-8662或1-888-743-0023；网址：www.oag.state.md.us。SAR Holdings Inc. d/b/a Sarku Japan位于30 Broad Street, 14th Floor, New York, NY 10004。

对于新墨西哥州居民，根据《公平信用报告法》享有权利，例如，当您的信用档案中的信息被用于对您不利的方面时您有权被告知，有权了解您的信用档案中的内容，有权询问您的信用评分，以及有权对不完整或不准确的信息提出异议。此外，根据《公平信用报告法》，消费者报告机构必须更正或删除不准确、不完整或无法核实的信息；消费者报告机构不得报告过时的负面信息；对您文件的访问受到限制；您必须同意向雇主提供信用报告；您可以限制根据您的信用报告中的信息获得的“预先筛选”信用和保险信息；并且您可以向违规者寻求损害赔偿。根据《公平信用报告法》，您可能拥有此处未概述的其他权利。根据《公平信用报告法》，身份盗窃受害者和现役军人拥有特定的额外权利。我们鼓励您通过访问www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf或写信给联邦贸易委员会消费者响应中心130-A室（600 Pennsylvania Ave. N.W., Washington D.C. 20580）。

对于纽约州居民，可联系纽约州总检察长：总检察长办公室（The Capitol, Albany, NY 12224-0341）；1-800-771-7755；或<https://ag.ny.gov/>。

对于北卡罗来纳州居民，可联系北卡罗来纳州总检察长：9001 Mail Service Center, Raleigh, NC 27699-9001；1-877-566-7226或1-919-716-6000；和www.ncdoj.gov。

对于罗德岛州居民，可联系罗德岛州总检察长：150 South Main Street, Providence, RI 02903；www.riag.ri.gov；和1-401-274-4400。根据罗德岛州法律，您有权获得有关此事件的任何警方报告。[共有十三（13）名罗德岛州居民受此事件影响。](#)