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

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

NOTICE OF DATA BREACH

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, 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

KROLL

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.

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

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

AVISO DE VIOLACIÓN DE DATOS

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

<<b2b_text_1(Variable State Holding Company)>>, haciendo negocios como Sarku Japan ("Sarku Japan") le escribe para informarle de un acontecimiento 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 Japón lanzó inmediatamente una investigación, con la ayuda de especialistas en ciberseguridad externos, para determinar la naturaleza y el alcance del evento. La investigación determinó que entre el 14 de enero 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 robada 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 una información personal que era 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 real o intentado de su información personal, le proporcionamos este aviso por precaución.

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

Lo que estamos haciendo. La confidencialidad, la privacidad y la seguridad de la información a nuestro cargo son algunas de nuestras más altas prioridades. Al enterarnos del evento, actuamos rápidamente para investigar y responder al evento, evaluar la seguridad de nuestros sistemas y notificar a las personas potencialmente afectadas. Estamos notificando a las personas potencialmente afectadas, incluido 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 evento pueda causar. Como precaución adicional, también ofrecemos servicios de monitorización de identidad a través de Kroll durante doce (12) meses, sin costo para usted.

Qué puede hacer. Le recomendamos que permanezca alerta contra incidentes de robo de identidad y fraude mediante la revisión de sus estados de cuenta y los informes crediticios 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 seguir para ayudar a proteger la información personal* adjuntos. Puede activar los servicios gratuitos de monitorización de identidad disponibles para usted. Las instrucciones de activación se adjuntan a esta carta.

Para obtener más información. Si tiene preguntas adicionales, llame a la línea de asistencia dedicada al 1-XXX-XXX-XXXX, de lunes a viernes de 8:00 a. m. a 5:30 p. m., hora central, excluyendo los principales festivos de EE. UU. Tenga su número de socio listo, que se puede encontrar en el *archivo adjunto*.

Atentamente,

Tony Chiu
Vicepresidente de finanzas y director financiero
Sarku Japan

Pasos que puede seguir para ayudar a proteger la información personal

ACTIVAR LA MONITORIZACIÓN DE LA IDENTIDAD

Para ayudar a recuperar la tranquilidad y restaurar la confianza después de este incidente, hemos asegurado los servicios de Kroll para proporcionarle una monitorización de identidad sin costo durante un año. Kroll es 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 monitorización de identidad incluyen monitorización de crédito, consulta de fraude y restauración de robo de identidad.

Visite **https://enroll.krollmonitoring.com** para activar y aprovechar sus servicios de monitorización de identidad.
*Tiene hasta el **4 de noviembre de 2022** para activar sus servicios de monitorización 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

KROLL

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

monitorización de crédito de para oficinas individuales

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 la 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 bajo la ley, asistencia con alertas de fraude e interpretar cómo se accede y usa la información personal, incluyendo 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 un robo de identidad, un investigador con licencia de Kroll y 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 Seguridad Social en su nombre y tener una dirección residencial de EE. UU. asociada con su archivo de crédito.

MONITORICE 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 gratuitamente 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 instalar una "alerta de fraude" inicial o extendida en un archivo de crédito sin costo alguno. Una alerta de fraude inicial es una alerta de 1 año que se instala 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 un robo de identidad, tiene derecho a una alerta de fraude extendida, la cual dura siete años. Si desea instalar 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 un bloqueo de crédito en un informe crediticio, lo cual prohibirá a una oficina de crédito divulgar datos del informe crediticio sin la autorización expresa del consumidor. El bloqueo de crédito está diseñado para evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. No obstante, debería ser consciente de que utilizar un bloqueo de crédito para tener el control de quién accede a la información personal y financiera de su informe crediticio 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 crediticia. Según la ley federal, no se le puede cobrar nada por realizar o levantar un bloqueo de crédito en su informe crediticio. Para solicitar un bloqueo 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 un bloqueo de crédito, póngase en contacto con las tres principales 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

Usted puede informarse acerca del robo de identidad, alertas de fraude, bloqueos 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); and 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 se ha retrasado por la aplicación de la ley.

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

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

NOTICE OF DATA BREACH

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, 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

KROLL

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.

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

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

数据泄露通知

尊敬的 <<First_Name>> <<Last_Name>>,

<<b2b_text_1(Variable State Holding Company)>> d/b/a Sarku Japan（ “Sarku Japan” ）
致函告知您可能会影响您的某些信息安全的事件。本通知将提供有关该事件的信息、我们的反应以及您可用于帮助保护您的信息免遭潜在滥用的资源（如您认为有必要）。

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访问某些Sarku Japan系统的权限，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。因此，我们对这些系统中的信息进行了彻底、深入的审查，以识别具有潜在可访问的个人信息的人员。2022年6月1日，我们完成了本次审查，以确认受影响数据的性质和范围以及与该数据相关的人员。虽然我们不知道是否有任何实际或企图滥用您的个人信息的情况，但出于谨慎之故，我们仍向您提供此通知。

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疑虑深表歉意。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。我们建议您不时查看您的账户对账单和信用报告，对身份盗窃和欺诈事件保持警觉，并及时向您的银行或金融机构报告任何可疑活动。随附的帮助保护个人信息所可采取的步骤中含有更多信息和资源。您可激活适用于您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 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，可在随附的附件中查找。

此致 ,

Tony Chiu
财务副总裁兼首席财务官
Sarku Japan

帮助保护个人信息所可采取的步骤激活身份监控

为了帮助缓解此次事件带来的疑虑并恢复信任，我们已获得Kroll的服务，在十二 (12) 个月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，足以帮助那些无意中暴露机密数据的人员。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 。
本函附有描述您的服务的更多信息。

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。如果您不能识别相关活动，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

您可以不受限地向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，解释个人信息如何获取和使用，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，专门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。

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，免费索取一份信用报告。

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，您则有权获得延长时限的欺诈警报，其为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

补充信息

您可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，以进一步了解身份盗窃、欺诈警报、安全冻结以及保护自己所可采取的措施。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。本通知不会因执法而延期。