Notice of Data Breach

August 3, 2022

A. Duda & Sons, Inc. and its affiliates and subsidiaries, including but not limited to Duda Farm Fresh Foods, Duda Ranches, DUDA Commercial Properties, The Viera Company, Viera Builders, and Duran Golf Club (collectively, "DUDA"), recently experienced a data security incident, and we are providing this notice to potentially affected individuals in compliance with applicable law. DUDA has always taken measures to protect the personal information it maintains and remains committed to helping affected individuals protect themselves to the best of the company's ability. Please read the below notice for more details and to see what steps you can take to help protect yourself.

What happened?
In June and July of 2022, an unauthorized third party used sophisticated security exploits to gain access to DUDA's information technology systems. On July 9, 2022, these cybercriminals deployed ransomware on DUDA's systems, encrypting most of DUDA's computer network. DUDA has since learned that, during this attack, the attackers also downloaded files from our systems that included personally identifiable information. DUDA reported the incident to law enforcement and has worked diligently to restore operations and security since the attack.

What information was involved?
The data accessed by the attackers was varied and substantial. In some cases, the information included full names, social security numbers, payroll data, financial information, dates of birth, email addresses, telephone numbers, addresses, employee identification numbers, employee dependent information, a combination of these data, or other data an individual may have provided to DUDA in the past. However, due to the volume of files taken and the nature of logging information, DUDA cannot determine with certainty the exact scope of personal information the attackers may have extracted.

To be safe, if you have provided personal information or data to DUDA or its affiliates in the past, you should assume that your personally identifiable information or data may have been compromised in this incident and take appropriate precautions.

What we are doing
DUDA has taken swift action to restore the functionality and security of its data systems following the attack. We are cooperating with law enforcement investigating the attack. DUDA is also working with outside consultants to strengthen our information security systems to reduce the risk of a similar attack in the future. We are offering certain credit monitoring services at no cost to individuals who are or who have a good faith belief that they have been affected by this incident. Further information on this offering is below.

What you can do
The most important thing you can do in response to this incident is to remain vigilant and

secure your financial and other accounts. Whether you have been affected by this specific breach or not, it is important to regularly review personal account statements and credit reports to ensure no unauthorized activity has occurred. Here are a few warning signs to help you determine whether your personal information may have been used by someone else:

- Receiving a bill for services or items you did not purchase
- Being contacted by a debt collector about debt you do not owe
- Seeing collection notices on your credit report that you do not recognize

Malicious actors may try to trick you into giving them more information using the compromised data. If you receive any suspicious communications, particularly regarding financial matters, you should verify the source of these communications before revealing any personal information. If you are threatened by anyone, you should contact law enforcement. If you believe you have been the victim of identity theft, you should also contact law enforcement, your state attorney general, or the Federal Trade Commission ("FTC").

You may want to change your passwords to various online accounts. If you do change your passwords, your new password should be substantially different from your old password to best ensure security. Remember, it is never a good idea to use the same password from work for your personal or household applications.

Additionally, you may also consider placing a security freeze on your credit report, as allowed by state law. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please note that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any request you make for new loans, credit, credit or debit cards, mortgages, employment, housing, or other services.

How to freeze your credit report
To place a security freeze on your credit report, you must contact each of the three major consumer reporting agencies individually: Equifax, Experian, and TransUnion. You can do this online, or in writing.

To do this online, you can go to each of these websites and create an account. You will need to set up a user ID and password with each agency.

If you prefer to contact the agencies in writing, you can send a security freeze request by regular, certified, or overnight mail to the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
1-800-909-8872

In order to request a security freeze in writing, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. The addresses where you have lived over the past 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, military identification, etc.)
7. If you are victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you elect to set up a security freeze online, the agencies may instead request an email address and telephone number for identity verification.

Identity theft resources
The Federal Trade Commission (FTC) is located at 600 Pennsylvania Avenue, NW Washington, DC 20580. If you believe you may have been a victim of identity theft, you may file a complaint with the FTC at www.ftc.gov/idtheft or by calling 1-877-ID-THEFT (877-438-4338).

You may also consider taking additional steps, which are outlined on the FTC's website: https://www.identitytheft.gov/. Here, you will find resources and a checklist of steps you can take to protect yourself.

State governments also provide resources on protecting yourself against identity theft. Some examples of these resources are listed below.

Florida Attorney General
Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399
1-866-966-7226

California Attorney General
P.O. Box 944255
Sacramento, CA 94244-2550
(800) 952-5225

North Carolina Attorney General
114 West Edenton Street
Raleigh, NC 27603
(919) 716-6400

Texas Attorney General
PO Box 12548
Austin, TX 78711-2548
(800) 621-0508

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
410-576-6300

Oregon Attorney General
1162 Court St. NE
Salem, OR 97301-4096
1-877-877-9392

How to sign up for credit monitoring services
In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score* services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: DUDASON8122. In order for you to receive the monitoring services described above, you must enroll on or before November 1, 2022.

As information relating to employees' dependents may have been included in the compromised data, we are also providing the parents of impacted minor dependents with access to Cyber Monitoring* services for you and your minor child for twenty-four (24) months at no charge. Cyber monitoring will look out for yours and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Cyber Monitoring* services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: DUDASON8222. Once you have enrolled yourself, click on your name in the top right corner and select Manage Family Protection. In the Family Protection area, click on "Add Child Monitoring", to add the information for the child that you are wanting to be included in the monitoring services. In order for you to receive the monitoring services described above, you must enroll by November 1, 2022.

For questions related to these offerings, please call Cyberscout's customer service line at 1-800-405-6108. Representatives are available until November 1, 2022, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

If you would like more information from DUDA, or have any questions, please email datasecurity@duda.com or call (407) 365-2035.

Services marked with an "" require an internet connection and email account and may not be available to minors under the age of 18 years of age; different services outlined in this correspondence are available for minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Aviso de violación de datos

3 de agosto de 2022

A. Duda & Sons, Inc. y sus afiliadas y subsidiarias, incluidas, entre otras, Duda Farm Fresh Foods, Duda Ranches, DUDA Commercial Properties, The Viera Company, Viera Builders y Duran Golf Club (colectivamente, "DUDA"), experimentaron recientemente un incidente de seguridad de datos, y estamos proporcionando este aviso a las personas potencialmente afectadas de conformidad con la ley aplicable. DUDA siempre ha tomado medidas para proteger la información personal que mantiene y mantiene su compromiso de ayudar a las personas afectadas a protegerse lo mejor que pueda la empresa. Lea el siguiente aviso para obtener más detalles y ver qué pasos puede tomar para ayudar a protegerse.

¿Qué sucedió?

En junio y julio de 2022, una identidad externa sin autorización utilizó seguridad sofisticada para obtener acceso a los sistemas de tecnología de la información de DUDA. El 9 de julio de 2022, estos ciberdelincuentes implementaron un secuestro de datos en los sistemas de DUDA, cifrado la mayor parte de la red informática de DUDA. Desde entonces, DUDA se enteró de que, durante este ataque, los atacantes también descargaron archivos de nuestros sistemas que incluían información de identificación personal. DUDA informó el incidente a las fuerzas del orden público y ha trabajado diligentemente para restaurar las operaciones y la seguridad desde el ataque.

¿Qué información estaba involucrada?

Los datos a los que accedieron los atacantes fueron variados y sustanciales. En algunos casos, la información incluía nombres completos, números de seguro social, datos de nómina, información financiera, fechas de nacimiento, direcciones de correo electrónico, números de teléfono, direcciones, números de identificación de empleados, información de dependientes de empleados, una combinación de estos datos u otros datos y persona pudo haber proporcionado a DUDA en el pasado. Sin embargo, debido al volumen de archivos tomados y la naturaleza de la información de registro, DUDA no puede determinar con certeza el alcance exacto de la información personal que los atacantes pueden haber extraído.

Para estar seguro, si ha proporcionado información o datos personales a DUDA o sus afiliados en el pasado, debe suponer que su información o datos de identificación personal pueden haberse visto comprometidos en este incidente y tomar las precauciones adecuadas.

Qué estamos haciendo

DUDA tomó medidas rápidas para restaurar la funcionalidad y la seguridad de sus sistemas de datos luego del ataque. Estamos cooperando con las fuerzas del orden que investigan el ataque. DUDA también está trabajando con consultores externos para fortalecer nuestros sistemas de seguridad de la información para reducir el riesgo de un ataque similar en el futuro. Estamos ofreciendo ciertos servicios de control de crédito sin costo alguno para las personas que creen de buena fe que han sido afectadas por este incidente. Más información sobre esta oferta se encuentra a continuación.

Lo que puedes hacer

Lo más importante que puede hacer en respuesta a este incidente es mantenerse alerta y proteger sus cuentas financieras y de otro tipo. Ya sea que se haya visto afectado por esta infracción específica o no, es importante revisar regularmente los estados de cuenta personales y los informes de crédito para asegurarse de que no se haya producido ninguna actividad no autorizada. Aquí hay algunas señales de advertencia para ayudarlo a determinar si su información personal puede haber sido utilizada por otra persona:

- Recibir una factura por servicios o artículos que no compró
- Ser contactado por un cobrador de deudas sobre una deuda que usted no debe
- Ver avisos de cobro en su informe de crédito que no reconoce

Las personas malintencionadas pueden engañarte para que les proporcione más información utilizando los datos comprometidos. Si recibe alguna comunicación sospechosa, particularmente sobre asuntos financieros, debe verificar la fuente de estas comunicaciones antes de revelar cualquier información personal. Si alguien lo amenaza, debe comunicarse con la policía. Si cree que ha sido víctima de un robo de identidad, también debe comunicarse con la policía, el fiscal general de su estado o la Comisión Federal de Comercio ("FTC").

Es posible que desee cambiar las contraseñas de varias cuentas en línea. Si cambia sus contraseñas, su nueva contraseña debe ser sustancialmente diferente de su contraseña anterior para garantizar mejor la seguridad. Recuerde, nunca es una buena idea usar la misma contraseña del trabajo para sus aplicaciones personales o domésticas.

Además, también puede considerar colocar un congelamiento de seguridad en su informe de crédito, según lo permita la ley estatal. Un congelamiento de seguridad prohíbe que una agencia de informes crediticios divulgue cualquier información del informe crediticio de un consumidor sin autorización por escrito. Tenga en cuenta que colocar un congelamiento de seguridad en su informe crediticio puede retrasar, interferir o impedir la aprobación oportuna de cualquier solicitud que realice para nuevos préstamos, tarjetas de crédito, crédito o débito, hipotecas, empleo, vivienda u otros servicios.

Cómo congelar su informe de crédito

Para colocar un congelamiento de seguridad en su informe crediticio, debe comunicarse individualmente con cada una de las tres principales agencias de informes crediticios: Equifax, Experian y TransUnion. Puede hacerlo en línea o por escrito.

Para hacer esto en línea, puede ir a cada uno de estos sitios web y crear una cuenta. Deberá configurar una identificación de usuario y una contraseña con cada agencia.

Si prefiere comunicarse con las agencias por escrito, puede enviar una solicitud de congelamiento de seguridad por correo regular, certificado o urgente a las siguientes direcciones:

Congelación de seguridad de Equifax
CORREOS. Casilla 105788
Atlanta, Georgia 30348
1-800-349-9960

Congelación de seguridad de Experian

CORREOS. Caja 9554
Allen, TX 75013
1-888-397-3742

Congelación de seguridad de TransUnion
Departamento de Asistencia a Víctimas de Fraude
CORREOS. Caja 6790
Fullerton, CA 92834
1-800-909-8872

Para solicitar un congelamiento de seguridad por escrito, deberá proporcionar la siguiente información:

1. Su 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. Las direcciones donde ha vivido durante los últimos cinco años
5. Comprobante de domicilio actual, como una factura actual de servicios públicos o de teléfono
6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir estatal o tarjeta de identificación, identificación militar, etc.)
7. Si es víctima de un robo de identidad, una copia de un informe policial, un informe de investigación o una denuncia ante una agencia del orden público en relación con el robo de identidad.

Si elige configurar un bloqueo de seguridad en línea, las agencias pueden solicitar una dirección de correo electrónico y un número de teléfono para verificar la identidad.

Recursos de robo de identidad

La Comisión Federal de Comercio (FTC) está ubicada en 600 Pennsylvania Avenue, NW Washington, DC 20580. Si cree que puede haber sido víctima de un robo de identidad, puede presentar una queja ante la FTC en www.ftc.gov/idtheft o llamando al 1-877-ID-THEFT (877-438-4338).

También puede considerar tomar medidas adicionales, que se describen en el sitio web de la FTC: https://www.identitytheft.gov/. Aquí encontrará recursos y una lista de verificación de los pasos que puede tomar para protegerse.

Los gobiernos estatales también brindan recursos para protegerse contra el robo de identidad. A continuación se enumeran algunos ejemplos de estos recursos.

Fiscal General de la Florida
Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399
1-866-966-7226

Fiscal General de California
P.O. Box 944255
Sacramento, CA 94244-2550

(800) 952-5225

Fiscal General de Carolina del Norte
114 West Edenton Street
Raleigh, NC 27603
(919) 716-6400

Fiscal General de Texas
PO Box 12548
Austin, TX 78711-2548
(800) 621-0508

Fiscal General de Maryland
200 St. Paul Place
Baltimore, MD 21202
410-576-6300

Fiscal General de Oregón
1162 Court St. NE
Salem, OR 97301-4096
1-877-877-9392

Cómo suscribirse a los servicios de monitoreo de crédito
En respuesta al incidente, le proporcionamos acceso a los servicios de Monitoreo de Crédito de Una Sola Oficina / Informe de Crédito de una Sola Oficina / Puntaje de Crédito de una Sola Oficina* sin cargo. Estos servicios le brindan alertas durante veinticuatro (24) meses a partir de la fecha de inscripción cuando se producen cambios en su archivo de crédito. Esta notificación se le envía el mismo día en que se realiza el cambio o la actualización con la oficina. Finalmente, le brindamos asistencia proactiva contra el fraude para ayudarlo con cualquier pregunta que pueda tener o en caso de que sea víctima de un fraude. Estos servicios serán proporcionados por Cyberscout, una empresa de TransUnion que se especializa en servicios de asistencia y reparación de fraudes.

Para inscribirse en los servicios de Monitoreo de crédito* sin cargo, inicie sesión en https://bfs.cyberscout.com/activate y siga las instrucciones proporcionadas. Cuando se le solicite, proporcione el siguiente código único para recibir servicios: DUDASON8122. Para que pueda recibir los servicios de monitoreo descritos anteriormente, debe inscribirse el 1 de noviembre de 2022 o antes.

Como la información relacionada con los dependientes de los empleados puede haber sido incluida en los datos comprometidos, también estamos proporcionando a los padres de los dependientes menores afectados acceso a los servicios de Cyber Monitoring* para usted y su hijos menor de edad durante veinticuatro (24) meses sin cargo. El monitoreo cibernético buscará sus datos personales y los de su hijo en la web oscura y lo alertará si su información de identificación personal o la de su hijo se encuentra en línea. Estos servicios serán proporcionados por Cyberscout, una compañía de TransUnion especializada en asistencia y servicios de remediación de fraude..

Para inscribirse en los servicios de Cyber Monitoring* sin cargo, inicie sesión en https://bfs.cyberscout.com/activate y siga las instrucciones proporcionadas. Cuando se le solicite, proporcione el siguiente código único para recibir servicios: DUDASON8222. Una vez que se haya inscrito, haga clic en su nombre en la esquina superior derecha y seleccione Administrar Protección familiar. En el área de Protección de la Familia, haga clic en "Agregar Monitoreo de Niños", para agregar la información del niño que desea que se incluya en los servicios de monitoreo. Para recibir los servicios de monitoreo descritos anteriormente, debe inscribirse antes del 1 de noviembre de 2022.

Si tiene preguntas relacionadas con estas ofertas, llame a la línea de atención al cliente de Cyberscout al 1-800-405-6108. Los representantes están disponibles hasta el 1 de noviembre de 2022 para ayudarlo con sus preguntas sobre este incidente, entre las 8:00 a. m. y las 8:00 p. m., hora del Este, de lunes a viernes. Llame al 1-800-405-6108 y proporcione al especialista en fraudes su código único mencionado anteriormente.

Si desea obtener más información de DUDA o tiene alguna pregunta, envíe un correo electrónico a datasecurity@duda.com o llame al (407) 365-2035.

Los servicios marcados con un "" requieren una conexión a Internet y una cuenta de correo electrónico y pueden no estar disponibles para menores de 18 años; Los diferentes servicios descritos en esta correspondencia están disponibles para menores de 18 años. Tenga en cuenta que al suscribirse a los servicios de monitoreo, se le puede solicitar que verifique la información personal para su propia protección para confirmar su identidad.