

# **EXHIBIT 1**

By providing this notice, Driscoll's Inc. ("Driscoll's") does not waive any rights or defenses regarding the applicability of California law, applicability of the California data event notification statute, or personal jurisdiction.

### **Nature of the Data Event**

On or about July 28, 2017, Driscoll's determined that some employees' payroll log-in credentials were compromised when the employees responded to a phishing email. Driscoll's launched an investigation and, with the help of a third-party forensic provider, later determined that some employees' email accounts had also been subject to unauthorized access as a result of the phishing email. The forensic investigator then reviewed the contents of these email accounts to determine whether they contained any sensitive personal information. On December 18, 2017, Driscoll's confirmed that sensitive information was located in one or more of the email accounts. On January 17, 2018, the forensic investigator completed the review of the affected email accounts and provided Driscoll's with a list of employees whose protected information was contained within the email accounts. The unauthorized access may have occurred between July 17, 2017 and August 18, 2017.

For a majority of the affected individuals, the data elements contained within the email account was the individual's name and Social Security number. For a small percentage of employees, the information contained within the email accounts about them was a combination of their name and one or more of Social Security number, driver's license number, Passport number, credit/debit card number, bank account information, medical information and health insurance information.

### **Notice to California Residents**

On February 9, 2018, Driscoll's will begin providing written notice of this incident to all potentially affected customers, which includes one thousand, three hundred and eighty-four (1,384) California residents. Written notice will be provided in substantially the same form as the letter attached hereto as *Exhibit A*.

### **Other Steps Taken and to Be Taken**

Upon discovering that protected information may have been subject to unauthorized access, Driscoll's moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

Driscoll's is providing all potentially affected individuals access to one year of free credit and identity monitoring services with AllClear ID. Additionally, Driscoll's is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. Driscoll's is also providing written notice of this incident to other state regulators as necessary.

# **EXHIBIT A**



Only the Finest Berries™

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00027  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

February 9, 2018

**Re: Notice of Data Breach**

Dear John Sample:

Driscoll's is writing to inform you of an incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

**What Happened?** On or about July 28, 2017, Driscoll's determined that some employees' payroll log-in credentials were compromised when the employees responded to a phishing email. Driscoll's launched an investigation and, with the help of a third-party forensic provider, later determined that some employees' email accounts had also been subject to unauthorized access as a result of the phishing email. The forensic investigator then reviewed the contents of these email accounts to determine whether they contained any sensitive personal information. On December 18, 2017, we confirmed that sensitive information was located in one or more of the email accounts. On January 17, 2018, the forensic investigator completed the review of the affected email accounts and provided Driscoll's with a list of employees whose protected information was contained within the email accounts. The unauthorized access may have occurred between July 17, 2017 and August 18, 2017.

**What Information Was Involved?** The information related to you that was contained within one of the email accounts included your name and Social Security number.

**What We Are Doing.** The confidentiality, privacy, and security of our employee information is one of our highest priorities. Driscoll's has stringent security measures in place to protect the security of information in our possession. In addition, as part of our ongoing commitment to the security of personal information in our care, we reset the passwords of all affected employees and are in the process of adding additional security measures.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-865-6896 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.



01-04-2-00

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) or by phone by calling 1-855-865-6896 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

***What You Can Do.*** You can review the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud.” You can also enroll to receive the free credit monitoring and identity restoration services described above.

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If you have any questions regarding this incident, you may call the confidential call center we have set for this matter at 1-855-865-6896 Monday through Saturday, 9:00 a.m. to 9:00 p.m. E.T.

Driscoll’s takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in cursive script that reads "Kate Terrell".

Kate Terrell  
Sr. VP, Chief Human Resources

## STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate this incident, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
<https://www.freeze.equifax.com>

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/](http://www.experian.com/freeze/)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/](http://www.transunion.com/)

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us). **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at [www.ncdoj.gov](http://www.ncdoj.gov). **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 agencies 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](http://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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.



Only the Finest Berries™

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00027  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

9 de febrero de 2018

**Ref.: Notificación de violación de los datos**

Estimado John Sample:

Driscoll's le escribe para informarle sobre un incidente que podría afectar la seguridad de su información personal. Tomamos este incidente con mucha seriedad y le brindamos la información y acceso a recursos para que pueda proteger su información personal, en caso de que considere apropiado hacerlo.

**¿Qué sucedió?** Alrededor del 28 de julio de 2017, Driscoll's determinó que los credenciales de ingreso a la nómina de sueldos de los empleados fueron comprometidos cuando los empleados respondieron a un mensaje electrónico conocido como "phishing". Driscoll's lanzó una investigación y con la ayuda de un proveedor forense externo, luego determinó que las cuentas de correo electrónico de algunos empleados también habían sido sujetas al acceso no autorizado como resultado de dicho mensaje electrónico. El investigador forense luego evaluó el contenido de estas cuentas de correo electrónico para determinar si contenían información personal sensible. El 18 de diciembre de 2017, confirmamos que información sensible se encontraba en una o más de las cuentas de correo electrónico. El 17 de enero de 2018, el investigador forense completó la evaluación de las cuentas de correo electrónico afectadas y entregó a Driscoll's una lista de los empleados cuya información protegida se encontraba dentro de las cuentas de correo electrónico. El acceso sin autorización podría haber ocurrido entre el 17 de julio de 2017 y el 18 de agosto de 2017.

**¿Qué información resultó involucrada?** La información relacionada con usted que se encontraba dentro de una de las cuentas de correo electrónico incluía su nombre y número del Seguro Social.

**¿Qué estamos haciendo.** La confidencialidad, privacidad y seguridad de la información de nuestros empleados es una de nuestras prioridades más importantes. Driscoll's ha adoptado estrictas medidas de seguridad para proteger la seguridad de la información en nuestro poder. Además, como parte de nuestro compromiso continuo con la seguridad de la información personal bajo nuestro cuidado, cambiamos las contraseñas de todos los empleados afectados y estamos tratando de agregar medidas adicionales de seguridad.

Como precaución adicional, hemos solicitado a AllClear ID que proteja su identidad durante 12 meses sin costo alguno para usted. Los siguientes servicios de protección de la identidad comienzan a partir de la fecha de esta notificación y usted puede usarlos en cualquier momento durante los próximos 12 meses.

AllClear Identity Repair: Este servicio está disponible para usted automáticamente y no requiere ningún tipo de inscripción. Si surge un problema, simplemente llame al 1-855-865-6896 y un investigador dedicado le ayudará a recuperar las pérdidas financieras, restaurar su crédito y asegurarse de que su identidad vuelve a su condición apropiada.



03-04-2



AllClear Fraud Alerts con Credit Monitoring: Este servicio ofrece la posibilidad de definir, renovar y remover alertas de fraude de 90 días en su archivo crediticio para ayudarlo a protegerse contra el fraude en el crédito. Además, brinda servicios de monitorización del crédito, un puntaje crediticio anual e informe crediticio por año y una póliza de seguro del robo de identidad de \$1 millón. Para inscribirse en este servicio, necesitará proveer su información personal a AllClear ID. Puede inscribirse en línea en [enroll.allclearid.com](http://enroll.allclearid.com) o por teléfono llamando al 1-855-865-6896 usando el siguiente código de rescate: Redemption Code.

Por favor, tome nota: Luego de la inscripción, se requieren pasos adicionales suyos para activar sus alertas telefónicas y alertas de fraude, y obtener su puntaje crediticio y archivo crediticio. Pasos adicionales también podrían requerirse para poder activar sus opciones de monitorización.

**Qué puede hacer.** Puede consultar la publicación adjunta “Pasos que puede tomar para prevenir el robo de identidad y fraude.” También puede inscribirse para recibir los servicios gratuitos de monitorización del crédito y restauración de la identidad que se describen más arriba.

**Para más información.** Entendemos que usted podría tener preguntas sobre este incidente que no se incluyen en esta carta. Si tiene alguna pregunta sobre este incidente, puede llamar al centro confidencial de llamadas que hemos creado para esta cuestión al 1-855-865-6896 de lunes a sábado de 9:00 a.m. a 9:00 p.m., hora del este.

Driscoll’s considera a la privacidad y seguridad de su información personal en nuestro poder con mucha seriedad. Lamentamos con sinceridad cualquier inquietud o inconveniente que este incidente le haya causado.

Atentamente,



Kate Terrell  
Vicepresidente Senior, Jefa de Recursos Humanos

## PASOS QUE PUEDE TOMAR PARA PREVENIR EL ROBO DE IDENTIDAD Y FRAUDE

Mientras continuamos investigando este incidente, usted puede tomar medidas directas para protegerse contra el posible robo de identidad y pérdida financiera.

Le aconsejamos que mantenga la vigilancia contra incidentes de robo de identidad y fraude, que evalúe sus estados de cuenta y que monitoree sus informes crediticios y formularios de explicación de beneficios por actividad sospechosa. Bajo las leyes de EE.UU., usted tiene derecho a un informe crediticio anual gratis de cada una de las tres empresas de informes de crédito más importantes. Para solicitar su informe crediticio gratis, visite [www.annualcreditreport.com](http://www.annualcreditreport.com) o llame gratis al 1-877-322-8228. También puede comunicarse directamente con las tres empresas crediticias más importantes para solicitar una copia gratis de su informe crediticio.

Sin cargo, puede pedir que estas empresas de informes de crédito coloquen un "alerta de fraude" a su archivo que alerta a los acreedores a tomar medidas adicionales para verificar su identidad antes de otorgar un crédito a su nombre. Note, sin embargo, que debido a que indica a los acreedores que deben cumplir ciertos procedimientos para protegerlo, también podría retrasar su capacidad de obtener un crédito mientras la agencia verifica su identidad. Ni bien una empresa de informes de crédito confirma su alerta del fraude, las otras son notificadas que deben colocar un alerta del fraude a su archivo. Si desea colocar un alerta del fraude, o tiene alguna pregunta sobre su informe crediticio, por favor comuníquese con una de las tres empresas que aparecen a continuación.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

También puede solicitar un congelamiento de sus informes crediticios. Un congelamiento de seguridad prohíbe que la empresa de informes crediticios comparta información del informe de crédito del consumidor sin la autorización escrita del consumidor. Sin embargo, tenga en cuenta que un congelamiento de seguridad a su informe crediticio podría retrasar, interferir o prevenir la aprobación oportuna de cualquier solicitud que presente por créditos nuevos, hipotecas, empleo, vivienda u otros servicios. Si ha sido víctima del robo de identidad y presenta a la empresa de informes crediticios una denuncia policial válida, no puede cobrarle por colocar, listar o levantar un congelamiento de seguridad. En todos los otros casos, la empresa de informes crediticios podrá cobrarle para colocar, cancelar transitoriamente o remover permanentemente un congelamiento de seguridad. Usted necesitará crear un congelamiento de seguridad diferente en cada una de las tres empresas principales de informes crediticios listadas más arriba si desea congelar todos sus archivos de crédito. Para obtener más información sobre cómo crear un congelamiento de seguridad, puede usar la siguiente información de contacto:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
<https://www.freeze.equifax.com>

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/](http://www.experian.com/freeze/)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/](http://www.transunion.com/)

También puede educarse sobre el robo de la identidad, las alertas de fraude y las medidas que puede tomar para protegerse, si se comunica con la Comisión Federal de Comercio o el Fiscal General de su estado. Se puede comunicar con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. **Los residentes de Maryland** se pueden comunicar con el Fiscal General en 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202, 1-888-0023, [www.oag.state.md.us](http://www.oag.state.md.us). **Los residentes de Carolina del Norte** se pueden comunicar con el Fiscal



General por correo al 9001 Mail Service Center, Raleigh, NC 27699-9001; llamando gratis al 1-877-566-7226; por teléfono al 1-919-716-6400; y en línea en [www.ncdoj.gov](http://www.ncdoj.gov). **Para los residentes de Nuevo México**, ustedes tienen derechos según la Ley de Informes Crediticios Justa, tales como el derecho a ser informados si la información en su archivo crediticio ha sido usada en su contra, el derecho a saber qué hay en su archivo crediticio, el derecho a pedir su puntaje crediticio y el derecho a disputar información incompleta o equivocada. Además, según la Ley de Informes Crediticios Justa, las agencias de informes del consumidor deben corregir o borrar información equivocada, incompleta o imposible de verificar; las agencias de informes del consumidor no pueden reportar información negativa vieja; el acceso a su archivo es limitado; debe prestar su consentimiento para que los informes crediticios sean provistos a empleadores; puede limitar ofertas “preevaluadas” de crédito y seguro que recibe según la información de su informe crediticio; y puede solicitar daños a quien los viole. Usted podría tener derechos adicionales según la Ley de Informes Crediticios Justos no resumidos aquí. Las víctimas de robo de identidad y personal militar en actividad tienen derechos adicionales específicos según la Ley de Informes Crediticios Justos. Le sugerimos que consulte sus derechos según la Ley de Informes Crediticios Justos visitando [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), o escribiendo a Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. La Comisión Federal de Comercio también sugiere a quienes descubren que su información ha sido usada equivocadamente que presenten una queja ante ellos. Las circunstancias de robo de identidad conocida o sospechada también deben ser informadas a las autoridades policiales. Esta notificación no ha sido retrasada por las autoridades policiales.



Only the Finest Berries™

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

February 9, 2018

**Re: Notice of Data Breach**

Dear John Sample:

Driscoll's is writing to inform you of an incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

**What Happened?** On or about July 28, 2017, Driscoll's determined that some employees' payroll log-in credentials were compromised when the employees responded to a phishing email. Driscoll's launched an investigation and, with the help of a third-party forensic provider, later determined that some employees' email accounts had also been subject to unauthorized access as a result of the phishing email. The forensic investigator then reviewed the contents of these email accounts to determine whether they contained any sensitive personal information. On December 18, 2017, we confirmed that sensitive information was located in one or more of the email accounts. On January 17, 2018, the forensic investigator completed the review of the affected email accounts and provided Driscoll's with a list of employees whose protected information was contained within the email accounts. The unauthorized access may have occurred between July 17, 2017 and August 18, 2017.

**What Information Was Involved?** The information related to you that was contained within one of the email accounts included your name and one or more of Social Security number, driver's license number, Passport number, credit/debit card number, bank account information, medical information and health insurance information.

**What We Are Doing.** The confidentiality, privacy, and security of our employee information is one of our highest priorities. Driscoll's has stringent security measures in place to protect the security of information in our possession. In addition, as part of our ongoing commitment to the security of personal information in our care, we reset the passwords of all affected employees and are in the process of adding additional security measures.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-865-6896 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.



01-04-1-00

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) or by phone by calling 1-855-865-6896 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

**What You Can Do.** You can review the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud.” You can also enroll to receive the free credit monitoring and identity restoration services described above.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have any questions regarding this incident, you may call the confidential call center we have set for this matter at 1-855-865-6896 Monday through Saturday, 9:00 a.m. to 9:00 p.m. E.T.

Driscoll’s takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in cursive script that reads "Kate Terrell".

Kate Terrell  
Sr. VP, Chief Human Resources

## STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate this incident, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
<https://www.freeze.equifax.com>

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/](http://www.experian.com/freeze/)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/](http://www.transunion.com/)

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us). **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at [www.ncdoj.gov](http://www.ncdoj.gov). **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 agencies 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](http://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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.



Only the Finest Berries™

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001  
ACD1234

00001  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

9 de febrero de 2018

**Ref.: Notificación de violación de los datos**

Estimado John Sample:

Driscoll's le escribe para informarle sobre un incidente que podría afectar la seguridad de su información personal. Tomamos este incidente con mucha seriedad y le brindamos la información y acceso a recursos para que pueda proteger su información personal, en caso de que considere apropiado hacerlo.

**¿Qué sucedió?** Alrededor del 28 de julio de 2017, Driscoll's determinó que los credenciales de ingreso a la nómina de sueldos de los empleados fueron comprometidos cuando los empleados respondieron a un mensaje electrónico conocido como "phishing". Driscoll's lanzó una investigación y con la ayuda de un proveedor forense externo, luego determinó que las cuentas de correo electrónico de algunos empleados también habían sido sujetas al acceso no autorizado como resultado de dicho mensaje electrónico. El investigador forense luego evaluó el contenido de estas cuentas de correo electrónico para determinar si contenían información personal sensible. El 18 de diciembre de 2017, confirmamos que información sensible se encontraba en una o más de las cuentas de correo electrónico. El 17 de enero de 2018, el investigador forense completó la evaluación de las cuentas de correo electrónico afectadas y entregó a Driscoll's una lista de los empleados cuya información protegida se encontraba dentro de las cuentas de correo electrónico. El acceso sin autorización podría haber ocurrido entre el 17 de julio de 2017 y el 18 de agosto de 2017.

**¿Qué información resultó involucrada?** La información relacionada con usted que se encontraba dentro de una de las cuentas de correo electrónico incluía su nombre y uno o más números del Seguro Social, número de la licencia de conductor, número de Pasaporte, número de tarjeta de crédito o débito, información de la cuenta bancaria, información médica e información del seguro de salud.

**¿Qué estamos haciendo.** La confidencialidad, privacidad y seguridad de la información de nuestros empleados es una de nuestras prioridades más importantes. Driscoll's ha adoptado estrictas medidas de seguridad para proteger la seguridad de la información en nuestro poder. Además, como parte de nuestro compromiso continuo con la seguridad de la información personal bajo nuestro cuidado, cambiamos las contraseñas de todos los empleados afectados y estamos tratando de agregar medidas adicionales de seguridad.

Como precaución adicional, hemos solicitado a AllClear ID que proteja su identidad durante 12 meses sin costo alguno para usted. Los siguientes servicios de protección de la identidad comienzan a partir de la fecha de esta notificación y usted puede usarlos en cualquier momento durante los próximos 12 meses.



03-04-1



AllClear Identity Repair: Este servicio está disponible para usted automáticamente y no requiere ningún tipo de inscripción. Si surge un problema, simplemente llame al 1-855-865-6896 y un investigador dedicado le ayudará a recuperar las pérdidas financieras, restaurar su crédito y asegurarse de que su identidad vuelve a su condición apropiada.

AllClear Fraud Alerts con Credit Monitoring: Este servicio ofrece la posibilidad de definir, renovar y remover alertas de fraude de 90 días en su archivo crediticio para ayudarlo a protegerse contra el fraude en el crédito. Además, brinda servicios de monitorización del crédito, un puntaje crediticio anual e informe crediticio por año y una póliza de seguro del robo de identidad de \$1 millón. Para inscribirse en este servicio, necesitará proveer su información personal a AllClear ID. Puede inscribirse en línea en [enroll.allclearid.com](http://enroll.allclearid.com) o por teléfono llamando al 1-855-865-6896 usando el siguiente código de rescate: Redemption Code.

Por favor, tome nota: Luego de la inscripción, se requieren pasos adicionales suyos para activar sus alertas telefónicas y alertas de fraude, y obtener su puntaje crediticio y archivo crediticio. Pasos adicionales también podrían requerirse para poder activar sus opciones de monitorización.

***Qué puede hacer.*** Puede consultar la publicación adjunta “Pasos que puede tomar para prevenir el robo de identidad y fraude.” También puede inscribirse para recibir los servicios gratuitos de monitorización del crédito y restauración de la identidad que se describen más arriba.

***Para más información.*** Entendemos que usted podría tener preguntas sobre este incidente que no se incluyen en esta carta. Si tiene alguna pregunta sobre este incidente, puede llamar al centro confidencial de llamadas que hemos creado para esta cuestión al 1-855-865-6896 de lunes a sábado de 9:00 a.m. a 9:00 p.m., hora del este.

Driscoll’s considera a la privacidad y seguridad de su información personal en nuestro poder con mucha seriedad. Lamentamos con sinceridad cualquier inquietud o inconveniente que este incidente le haya causado.

Atentamente,



Kate Terrell  
Vicepresidente Senior, Jefa de Recursos Humanos

## PASOS QUE PUEDE TOMAR PARA PREVENIR EL ROBO DE IDENTIDAD Y FRAUDE

Mientras continuamos investigando este incidente, usted puede tomar medidas directas para protegerse contra el posible robo de identidad y pérdida financiera.

Le aconsejamos que mantenga la vigilancia contra incidentes de robo de identidad y fraude, que evalúe sus estados de cuenta y que monitorice sus informes crediticios y formularios de explicación de beneficios por actividad sospechosa. Bajo las leyes de EE.UU., usted tiene derecho a un informe crediticio anual gratis de cada una de las tres empresas de informes de crédito más importantes. Para solicitar su informe crediticio gratis, visite [www.annualcreditreport.com](http://www.annualcreditreport.com) o llame gratis al 1-877-322-8228. También puede comunicarse directamente con las tres empresas crediticias más importantes para solicitar una copia gratis de su informe crediticio.

Sin cargo, puede pedir que estas empresas de informes de crédito coloquen un "alerta de fraude" a su archivo que alerta a los acreedores a tomar medidas adicionales para verificar su identidad antes de otorgar un crédito a su nombre. Note, sin embargo, que debido a que indica a los acreedores que deben cumplir ciertos procedimientos para protegerlo, también podría retrasar su capacidad de obtener un crédito mientras la agencia verifica su identidad. Ni bien una empresa de informes de crédito confirma su alerta del fraude, las otras son notificadas que deben colocar un alerta del fraude a su archivo. Si desea colocar un alerta del fraude, o tiene alguna pregunta sobre su informe crediticio, por favor comuníquese con una de las tres empresas que aparecen a continuación.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

También puede solicitar un congelamiento de sus informes crediticios. Un congelamiento de seguridad prohíbe que la empresa de informes crediticios comparta información del informe de crédito del consumidor sin la autorización escrita del consumidor. Sin embargo, tenga en cuenta que un congelamiento de seguridad a su informe crediticio podría retrasar, interferir o prevenir la aprobación oportuna de cualquier solicitud que presente por créditos nuevos, hipotecas, empleo, vivienda u otros servicios. Si ha sido víctima del robo de identidad y presenta a la empresa de informes crediticios una denuncia policial válida, no puede cobrarle por colocar, listar o levantar un congelamiento de seguridad. En todos los otros casos, la empresa de informes crediticios podrá cobrarle para colocar, cancelar transitoriamente o remover permanentemente un congelamiento de seguridad. Usted necesitará crear un congelamiento de seguridad diferente en cada una de las tres empresas principales de informes crediticios listadas más arriba si desea congelar todos sus archivos de crédito. Para obtener más información sobre cómo crear un congelamiento de seguridad, puede usar la siguiente información de contacto:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
<https://www.freeze.equifax.com>

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/](http://www.experian.com/freeze/)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/](http://www.transunion.com/)

También puede educarse sobre el robo de la identidad, las alertas de fraude y las medidas que puede tomar para protegerse, si se comunica con la Comisión Federal de Comercio o el Fiscal General de su estado. Se puede comunicar con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. **Los residentes de Maryland** se pueden comunicar con el Fiscal General en 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202, 1-888-0023, [www.oag.state.md.us](http://www.oag.state.md.us). **Los residentes de Carolina del Norte** se pueden comunicar con el Fiscal



General por correo al 9001 Mail Service Center, Raleigh, NC 27699-9001; llamando gratis al 1-877-566-7226; por teléfono al 1-919-716-6400; y en línea en [www.ncdoj.gov](http://www.ncdoj.gov). **Para los residentes de Nuevo México**, ustedes tienen derechos según la Ley de Informes Crediticios Justa, tales como el derecho a ser informados si la información en su archivo crediticio ha sido usada en su contra, el derecho a saber qué hay en su archivo crediticio, el derecho a pedir su puntaje crediticio y el derecho a disputar información incompleta o equivocada. Además, según la Ley de Informes Crediticios Justa, las agencias de informes del consumidor deben corregir o borrar información equivocada, incompleta o imposible de verificar; las agencias de informes del consumidor no pueden reportar información negativa vieja; el acceso a su archivo es limitado; debe prestar su consentimiento para que los informes crediticios sean provistos a empleadores; puede limitar ofertas “preevaluadas” de crédito y seguro que recibe según la información de su informe crediticio; y puede solicitar daños a quien los viole. Usted podría tener derechos adicionales según la Ley de Informes Crediticios Justos no resumidos aquí. Las víctimas de robo de identidad y personal militar en actividad tienen derechos adicionales específicos según la Ley de Informes Crediticios Justos. Le sugerimos que consulte sus derechos según la Ley de Informes Crediticios Justos visitando [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), o escribiendo a Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. La Comisión Federal de Comercio también sugiere a quienes descubren que su información ha sido usada equivocadamente que presenten una queja ante ellos. Las circunstancias de robo de identidad conocida o sospechada también deben ser informadas a las autoridades policiales. Esta notificación no ha sido retrasada por las autoridades policiales.