Additional 19936

PERKINS & CO

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-933-1103
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

May 4, 2021

Dear <<FirstName>> <<LastName>>:

Perkins & Co (Perkins) is writing to notify you about a recent cybersecurity incident involving our third-party data hosting vendor, Netgain, that may affect the security of some of your personal information. We take this event and the security of your personal information very seriously and this letter provides steps you may take to better protect against potential misuse of your information should you feel it is necessary. If you have questions about the event, please call our dedicated call center at 1-833-933-1103, available Monday through Friday, 6am to 6pm Pacific Time.

We confirmed that Netgain has taken steps to further safeguard against future threats, including implementing additional advanced threat protection tools, resetting passwords, reviewing and restricting access rights, and hardening network security rules and protocols. Further, Perkins is retaining an expert consultant to help provide our firm and clients with an even higher level of data security. Perkins reported this incident to the IRS and state tax authorities, as well as applicable state data privacy regulatory authorities.

As an added precaution, we are offering complimentary access to twenty-four (24) months of credit monitoring and identity theft restoration services through IDX. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one (1) free credit report annually from each of the three (3) major credit reportin bureaus. To ordery our free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three (3) major credit bureaus directly to request a free copy of your credit report.

Place a Security Freeze

You have the right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, 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. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

To remove the security freeze, you must send a written request to each of the three (3) credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Place a Fraud Alert

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert is a one-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 (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/ fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/ credit-report-services

Additional Information

Under Massachusetts law, you have the right to obtain any police report filed regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, your state Attorney General or the Federal Trade Commission. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; (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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should be reported to law enforcement, the FTC, and the Massachusetts Attorney General.

We understand that you may have questions about this event not addressed in this letter. If you have additional questions, please call our dedicated call center at 1-833-933-1103, available Monday through Friday, 6am to 6pm Pacific Time.

Sincerely,

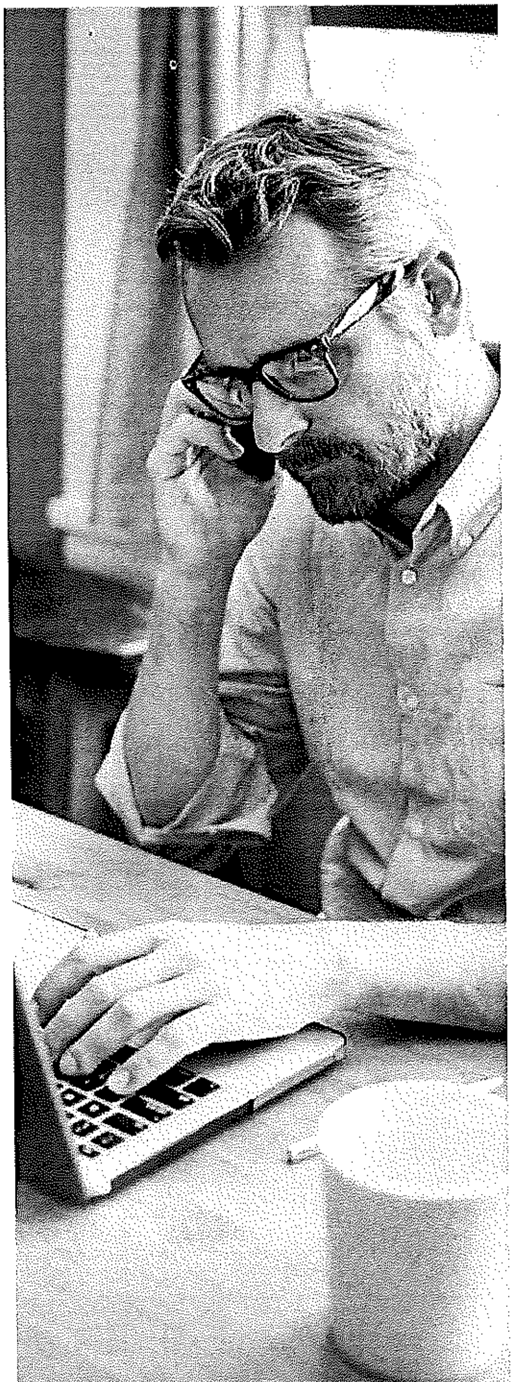
Jared Holum, President
Perkins & Co

Enroll in Complimentary Credit Monitoring

1. Website and Enrollment. We are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twenty-four (24) months of tri-bureau credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-933-1103 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. Please note, the deadline to enroll is August 4, 2021.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

John Hancock



Safeguarding your information is our top priority

John Hancock backs you up with a Cybersecurity Guarantee when you apply and follow these online safeguards!

John Hancock takes the protection of your account seriously. As part of our commitment in continuing to provide you with an easy, safe and secure way to access your retirement account online, here are the security safeguards that we require you to follow when creating or updating your account profile.

Is your account profile up-to-date?

Username

- A username uniquely identifies you and your account.
- Pick a username that is personal to you and difficult for others to guess. This should be something only you know.
- Do not use your Social Security number (SSN).

Password

- Create a unique and strong password that will be hard for others to figure out.
- Pick a random combination of upper and lowercase letters, numbers and special characters (e.g. @, #, ^, %) that's at least 8 characters long.
- Consider using a passphrase (and not dictionary words) - a short phrase that's easy for you to recall and strengthen using only the first letter of each word in the phrase and adding special characters. For example, 'I like toast and eggs for breakfast on weekends' can be changed to 'Ilt&e4bow'.

Questions about security?

One-on-one support
800.294.3575
Contact us if you need assistance updating your profile or want to learn more about account security.

In an age where people share so much personal information on social media, blogs, and websites, it can be a challenge to pick unique IDs, passwords, and questions that are only known to you.

Remember you can always update your personal and account security information by clicking on 'My Profile' when you log into the website.

Recommended browsers:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari (Mac)

Also, keep in mind the following:

- Don't use common words (e.g. water, car) or any personal information.
- Don't use the same password for multiple websites – create a unique password for each of your critical websites. Once a password is compromised at one site, it's easy for someone to try that same password for other sites.
- Don't use your username for your password – these should always differ.
- Don't share your password with anyone – including family members.
- Change your password immediately if you are a victim of identity theft.

Better security takes more than a username and password

Security question and answer

- Pick a question with an answer that is relevant to you but only known to you.
- The answer to your security question is needed to reset your username or password online, so choose a question with a concise answer that only you can easily recall.
- For security purposes, never share your security question with anyone.

Mobile phone number and email address

To enhance security further, you are required to add a mobile phone number and personal (non-work) email address to your account profile. This allows us to send you security-related messages when a transaction or update occurs on your account to confirm it was actually initiated by you. If you don't recognize the transaction, contact us immediately so we can act quickly to protect your account.

There's also an authentication protocol that occurs when you are logging into your online account. Any visit to the website that doesn't pass this authentication protocol will result in us sending you a security code to your email or phone number on file that you must input to complete the login process.

As well, transactions to update certain personal information or to request a distribution (withdrawal or loan) from your account online will go through additional security protocols to help identify fraudulent activity. In these situations, we will send a security code to the personal email address or mobile number we have on file for you. You will then have a limited amount of time to enter that code into the site to authorize and confirm that transaction.

Additional protocols help protect your account

We have procedures in place to protect your account. For example, under certain conditions,when you request a distribution (loan or withdrawal) a 10-calendar day cooling period (or hold) may apply.

Browser security

John Hancock protects our systems, data, and our clients' information by enforcing access to our websites with a minimum 256-bit(SSL/TLS) encryption; only secure connections will be allowed access through to the authentication page.

Therefore, we recommend you use a browser that supports 256-bit encryption, is JavaScript enabled, and accepts cookies. These requirements help ensure the safety of your financial information and allow us to track usage of the site in order to improve our service to you.

If your browser does not support 256-bit encryption, click on one of the links to update your browser. The latest versions of Internet Explorer, Mozilla Firefox, Google Chrome, or Safari offer 256-bit encryption as a standard feature.

John Hancock's Cybersecurity Guarantee – our promise to you!

At John Hancock, your trust and the security of your account is important to us. By doing your part in keeping your John Hancock accounts safe online, we will back you up with a Cybersecurity Guarantee.

For more information, read the attached **Cybersecurity Guarantee Certificate**.

One-on-one support
800.294.3575
Representatives are available between 8 a.m. and 10 p.m. Eastern time on New York Stock Exchange business days. For your protection, all calls to a representative are recorded.

Do these to help keep you safe online...

- Fraudsters are out there looking for user credentials to steal. They are looking to impersonate people or organizations in order to trick you into disclosing sensitive information. Methods can include shoulder surfing, social engineering, and simple guessing based on online profile information (Facebook, LinkedIn, etc). So make it as difficult and time consuming as possible for others to guess your credentials.
- When logging into a website with your personal credentials, type in the web address in the browser yourself, rather than clicking on a link from an email or a search engine. Look for signals that a website is secure, such as a URL that begins with "https" ("s" stands for secure).
- Be wary of emails you do not recognize or that look suspicious as they could be phishing attempts.
- Be cautious about opening attachments or downloading files, regardless of who sent them.
- Don't send personal or financial information via email or text.
- Review your statements or transaction details as soon as you receive them. If you notice anything unusual or your statement is late in coming, contact us to confirm your profile information and account balances.
- Become 'malware-aware' and stay away from shady websites so your computer/device does not become infected. Make sure you are on the right site!
- Always update your web browser and use the latest versions of Internet Explorer, Firefox, Google Chrome, or Safari.
- Install anti-virus and malware protection software on your home computer and enable automatic updates.
- Download operating system and software updates only from trusted sources.
- If you have broadband or an 'always on' Internet connection, enable firewall software on your computer.
- Don't select 'Remember Passwords' in your browser.
- Understand the risks of using free Wifi hotspots.

Visit us online at **johnhancock.com/myplan**

John Hancock's Cybersecurity Guarantee in full is available at JHRPS.com/CybersecurityGuarantee-OA

John Hancock Retirement Plan Services, LLC offers administrative or recordkeeping services to sponsors and administrators of retirement plans, as well as a platform of investment alternatives that is made available without regard to the individualized needs of any plan. Unless otherwise specifically stated in writing, John Hancock Retirement Plan Services, LLC does not, and is not undertaking to, provide impartial investment advice or give advice in a fiduciary capacity. John Hancock Trust Company LLC provides trust and custodial services to such plans.

JH Enterprise® is a registered trademark of John Hancock Life Insurance Company (U.S.A.).

NOT FDIC INSURED. MAY LOSE VALUE. NOT BANK GUARANTEED.

John Hancock

Cybersecurity Guarantee

John Hancock backs up your retirement account with a Cybersecurity Guarantee. If someone takes cash from your covered account[1] through no fault of your own, John Hancock will reimburse your account the amount of cash taken.[2]

TO BECOME ELIGIBLE FOR JOHN HANCOCK'S CYBERSECURITY GUARANTEE:

FOLLOW PRUDENT ONLINE SECURITY PRACTICES[3] and maintain up-to-date contact information with us, so we can contact you if we suspect unauthorized activity.

- Never share your account access information, including username, password, and answers to security questions.
- Use unique and strong usernames and passwords for your John Hancock accounts, and change your password immediately if you're a victim of identity theft.
- Remain current with security protections on your email, accounts, and devices, including antispyware and antivirus software, changing passwords when accounts may be compromised, and enabling automatic updates.

NOTIFY US IMMEDIATELY AT 800-294-3575 if you're a victim of identity theft or if you suspect unauthorized activity in your retirement account.

- Regularly monitor your account for unusual activity, promptly reviewing written and electronic correspondence, account statements, and confirmations as they're made available to you.
- Notify us within 30 days that you intend to make a claim pursuant to this Cybersecurity Guarantee.

COOPERATE IN GOOD FAITH with any investigation.

- We may ask you to take follow-up actions, such as having a professional computer security company clean your computer hard drive or asking you to file a police report, provide an affidavit, or sign a release.
- John Hancock will determine the applicability of the Cybersecurity Guarantee and any amounts due to you.

OUR SIGNATURE IS BEHIND IT.

1 "Covered accounts" include your retirement accounts with John Hancock, such as a 401(k) or profit-sharing plan, for which John Hancock Retirement Plan Services, LLC is the recordkeeper. 2 See Guarantee, available at johnhancock.com/myplan, for full eligibility requirements. 3 Recommended online security practices are available at johnhancock.com/myplan.

MS-P 37374-GE 02/20 41526

MS020320508599 | 19244

PERKINS & CO

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-933-1103
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

May 4, 2021

Dear <<FirstName>> <<LastName>>:

Perkins & Co (Perkins) is writing to notify you about a recent cybersecurity incident involving our third-party data hosting vendor, Netgain, that may affect the security of some of your personal information. We take this event and the security of your personal information very seriously and this letter provides steps you may take to better protect against potential misuse of your information should you feel it is necessary. If you have questions about the event, please call our dedicated call center at 1-833-933-1103, available Monday through Friday, 6am to 6pm Pacific Time.

We confirmed that Netgain has taken steps to further safeguard against future threats, including implementing additional advanced threat protection tools, resetting passwords, reviewing and restricting access rights, and hardening network security rules and protocols. Further, Perkins is retaining an expert consultant to help provide our firm and clients with an even higher level of data security. Perkins reported this incident to the IRS and state tax authorities, as well as applicable state data privacy regulatory authorities.

As an added precaution, we are offering complimentary access to twenty-four (24) months of credit monitoring and identity theft restoration services through IDX. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three (3) major credit bureaus directly to request a free copy of your credit report.

Place a Security Freeze
You have the right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, 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. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

To remove the security freeze, you must send a written request to each of the three (3) credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Place a Fraud Alert

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert is a one-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 (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

Under Massachusetts law, you have the right to obtain any police report filed regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, your state Attorney General or the Federal Trade Commission. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; (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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should be reported to law enforcement, the FTC, and the Massachusetts Attorney General.

We understand that you may have questions about this event not addressed in this letter. If you have additional questions, please call our dedicated call center at 1-833-933-1103, available Monday through Friday, 6am to 6pm Pacific Time.

Sincerely,

Jared Holum, President
Perkins & Co

Enroll in Complimentary Credit Monitoring

1. Website and Enrollment. We are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twenty-four (24) months of tri-bureau credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-933-1103 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. Please note, the deadline to enroll is August 4, 2021.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

PERKINS & CO

A la atención de IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

Para inscribirse, llame al:
1-833-933-1103
O visite:
https://app.idx.us/account-creation/protect
Código de inscripción:
<<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

4 de mayo de 2021

Estimado <<FirstName>> <<LastName>>:

Perkins & Co (Perkins) le escribe para notificarle acerca de un incidente reciente en la seguridad cibernética que involucra a nuestro proveedor de alojamiento de datos externo, Netgain, que puede afectar la seguridad de parte de su información personal. Tomamos con mucha seriedad este suceso y la seguridad de su información personal, y esta carta le proporciona las medidas que puede tomar para contar con mayor protección contra el posible uso indebido de su información si lo considera necesario. Si tiene preguntas acerca de este suceso llame a nuestro centro de atención dedicado al 1-833-933-1103, disponible de lunes a viernes de 6 a. m. a 6 p. m. hora del Pacífico.

Confirmamos que Netgain ha tomado medidas para brindar mayor protección contra las futuras amenazas, incluida la implementación de herramientas adicionales de avanzada para la protección contra amenazas, el reseteo de contraseñas, la revisión y restricción de derechos de acceso, y el recrudecimiento de las reglas y los protocolos de seguridad de la red. Además, Perkins mantiene un asesor experto para poder brindar a la empresa y a nuestros clientes un nivel incluso mayor de seguridad de datos. Perkins informó acerca de este incidente a las autoridades fiscales estatales y del Servicio de Impuestos Internos (IRS), así como las autoridades normativas de privacidad de datos de los estados pertinentes.

Como precaución añadida, le ofrecemos acceso de cortesía a veinticuatro (24) meses de servicios de control de crédito y restauración contra el robo de identidad a través de IDX. Las personas que deseen recibir estos servicios deben inscribirse. Para hacerlo, deben seguir las instrucciones de inscripción adjuntas.

Le recomendamos que esté atento contra incidentes de fraude y robo de identidad, que revise sus estados de cuenta y supervise sus informes de crédito en busca de actividad sospechosa. Conforme a la ley de EE. UU., usted tiene derecho a un (1) informe anual gratuito de crédito de cada una de las tres (3) principales agencias de informe de crédito. Para solicitar su informe de crédito gratuito, visite www.annualcreditreport.com o llame sin cargo al 1-877-322-8228. También puede comunicarse con las tres (3) principales oficinas de crédito directamente para solicitar una copia gratuita de su informe de crédito.

Coloque un congelamiento de seguridad

Usted tiene derecho a colocar un congelamiento de seguridad en su informe de crédito, que le prohibirá a una agencia de informe del consumidor divulgar información de su informe de crédito sin su autorización expresa. El congelamiento de seguridad está diseñado para evitar la aprobación de créditos, préstamos y servicios en su nombre sin su consentimiento. Sin embargo, usted debe estar al tanto de que el uso del congelamiento de seguridad para controlar quién obtiene acceso a la información personal y financiera de su informe de crédito puede demorar, interferir o prohibir la aprobación puntual de cualquier posterior solicitud o pedido que haga en relación con un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta que involucre la extensión de crédito. Conforme a la ley federal, no se le puede cobrar por colocar ni retirar un congelamiento de seguridad en su informe de crédito. Si desea colocar un congelamiento de seguridad. comuníquese con las principales agencias de informe del consumidor enumeradas a continuación:

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

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

1. Su nombre completo (incluida la inicial del segundo nombre, así como también Jr., Sr., II, III, etc.).
2. Número de seguro social.
3. Fecha de nacimiento.
4. Si se mudó en los últimos cinco (5) años, proporcione las direcciones en las que haya vivido durante los últimos cinco (5) años.
5. Prueba de su dirección actual, tal como factura telefónica o de los servicios actuales.
6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (identificación o licencia de conducir estatal, identificación militar, etc.).
7. Si usted es víctima de robo de identidad, incluya una copia del informe policial, informe de la investigación o queja a un organismo encargado de hacer cumplir la ley en relación con el robo de identidad.

Las agencias de informe de crédito tienen uno (1) a tres (3) días hábiles después de recibir su solicitud para colocar un congelamiento de seguridad en su informe de archivo crediticio, conforme al método de solicitud. Las oficinas de crédito también deben enviarle una confirmación por escrito dentro de los cinco (5) días hábiles y brindarle el proceso por el cual usted puede retirar el congelamiento de seguridad, incluido un mecanismo de autenticación. Tras recibir una solicitud directa de su parte para retirar un congelamiento de seguridad y tras recibir la identificación apropiada de su parte, la agencia de informe del consumidor deberá eliminar un congelamiento de seguridad dentro del término de una (1) hora tras recibir la solicitud por teléfono del retiro o dentro de los tres (3) días hábiles tras recibir la solicitud por correo del retiro.

Para retirar el congelamiento de seguridad, debe enviar una solicitud por escrito a cada una de las tres (3) oficinas de crédito por correo e incluir la identificación apropiada (nombre, dirección y número de seguro social) y número de PIN o contraseña que se le proporcionaron cuando colocó el congelamiento de seguridad. Las oficinas de crédito tienen tres (3) días hábiles tras recibir su solicitud para retirar el congelamiento de seguridad.

Coloque un alerta de fraude

Como alternativa a un congelamiento de seguridad, tiene derecho a colocar un alerta de fraude inicial o extendido en su archivo sin costo. Un alerta de fraude inicial es un alerta de un año que se coloca en el expediente de crédito de un consumidor. Tras visualizar un alerta de fraude en el expediente de crédito de un consumidor, se requiere a una empresa que tome las medidas para verificar la identidad del consumidor antes de extender un nuevo crédito. Si usted es víctima de robo de identidad, tiene derecho a recibir un alerta de fraude extendido, lo que es un alerta de fraude que dura siete (7) años. Si desea colocar un alerta de fraude, comuníquese con alguna de las agencias enumeradas a continuación:

Experian	TransUnion	Equifax
P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Información adicional

Conforme a la ley de Massachusetts, usted tiene derecho a presentar cualquier informe policial en relación con dicho incidente. Si usted es víctima de robo de identidad, también tiene derecho a presentar un informe policial y obtener una copia de este.

Puede obtener más información en relación con el robo de identidad, los alertas de fraude, los congelamientos de seguridad y las medidas que puede tomar para protegerse al contactar a las agencias de informe del consumidor, el Fiscal general de su estado o la Comisión Federal de Comercio. Puede ponerse en contacto con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también alienta a aquellos que detectan que su información se ha usado indebidamente a presentar una queja ante ellos. También puede obtener más información sobre cómo presentar dicha queja por medio de la información de contacto enumerada anteriormente. Las instancias de robo de identidad conocidas o bajo sospecha deben informarse al organismo de cumplimiento de la ley, la Comisión Federal de Comercio (FTC) y el Fiscal general de Massachusetts.

Entendemos que usted puede tener preguntas acerca de este suceso que no se aborden en esta carta. Si tiene más preguntas, llame a nuestro centro de atención dedicado al 1-833-933-1103, disponible de lunes a viernes de 6 a. m. a 6 p. m. hora del Pacífico.

Atentamente,

Jared Holum, Presidente
Perkins & Co

Inscríbase en el control de crédito de cortesía

1. Sitio web e inscripción. Estamos ofreciendo servicios de protección contra el robo de identidad a través de IDX, firma experta de servicios de recuperación y violación de datos. Los servicios de protección de identidad de IDX incluyen: veinticuatro meses (24) de supervisión mediante CyberScan y de crédito a través de tres oficinas, una póliza de reembolso de seguro de $1.000.000, y servicios de recuperación por robo de identidad totalmente gestionados. Con esta protección, IDX le ayudará a solucionar problemas si su identidad se ve comprometida. Le recomendamos que se ponga en contacto con IDX si tiene alguna pregunta y que se inscriba en los servicios de protección de identidad gratuitos al teléfono 1-833-933-1103 o visite https://app.idx.us/account-creation/protect y use el Código de inscripción suministrado anteriormente. Tenga en cuenta que la fecha límite para la inscripción es el 4 de agosto de 2021.

2. Active el control de crédito proporcionado como parte de su afiliación a la protección de la identidad de IDX. El control incluido en la afiliación debe activarse para ser efectivo. Nota: Debe tener crédito establecido y acceso a una computadora y a Internet para usar este servicio. Si necesita asistencia, IDX podrá ayudarle.