



*Leading the world in quality lift truck
attachments, forks and accessories.*

cascade[®]
corporation

April 1, 2021

Re: Notice of Data Breach

Dear Cascade Current or Former Employee:

Cascade Corporation (Cascade) is writing to inform you of a recent cybersecurity incident involving a Cascade vendor called Perkins & Co (Perkins) that provides services associated with your Cascade 401(k) plan account. This incident that may impact the security of your personal information.

Cascade sent you a preliminary communication about this incident in January, 2021. Since then, Perkins has provided new information to Cascade, which Cascade is now providing you through this letter. This letter also contains details about credit monitoring assistance that is available to you.

Although Perkins informed Cascade that it is unaware at this time of any actual or attempted misuse of your personal information, Cascade is providing you with details about the incident, Perkins' response, and steps you can take to better protect your personal information, should you feel it appropriate to do so.

Who is Perkins & Co / Why Does Perkins Have My Information? Perkins provides audit services to the employee benefit plan of Cascade. As part of those services, Perkins handles information relating to Cascade employee and benefits plan participants' personal information, including your personal information. This cybersecurity incident occurred with Netgain, Perkins' third-party data hosting vendor. **Please know that this incident did not impact the computer systems of Cascade.**

What Happened? According to Perkins, on December 3, 2020, Netgain alerted Perkins that they had shut down their systems and began working with outside cybersecurity specialists because of a ransomware attack on their systems that impacted Perkins' normal business operations.

On January 15, 2021, Netgain confirmed the following to Perkins: Between November 8, 2020 and December 3, 2020, an attacker accessed servers storing Perkins' client files, some of which they copied and stole. They also encrypted files and demanded to be paid a ransom by Netgain in exchange for returning copies of stolen files and providing a key to access encrypted files. Netgain paid a ransom and the attacker returned the files they had stolen, along with a decryption key. According to Perkins and Netgain, law enforcement and the cybersecurity specialists they engaged indicated that this attacker is not known to post the data, nor keep any copies of it once a ransom is paid. However, we know that there are no guarantees, and we still consider any data viewed or stolen by the attacker to be at risk.

2201 NE 201st Avenue
Fairview, OR 97024-9718
PO Box 20187
Portland, OR 97294-0187
800 CASCADE (227.2233)
503.669.6300
Fax 503.669.6716
www.cascorp.com



What Information Was Involved? According to Perkins, data relating to the employee benefit plan audit was stored on a server that Netgain reports was accessed by the attacker, though there is no indication Perkins or Cascade was intentionally targeted in this attack. Due to your status as a plan participant or current/former employee of Cascade, Perkins believes the following types of your personal information may have been viewed and/or stolen by the attacker: name, Social Security number, employee identification number, date of birth, and benefit/retirement plan account information.

What Cascade is Doing. Cascade takes the security and privacy of the personal information entrusted to us very seriously. In addition to the actions addressed above, Perkins informed Cascade that it has partnered with an outside "data mining" vendor to determine precisely what and whose personal information may have been impacted by this incident. Perkins informed Cascade 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 Perkins and its clients with an even higher level of data security. Perkins reported this incident to applicable state data privacy regulatory authorities.

As an added precaution, **Perkins is offering you access to complimentary credit monitoring and identity restoration services** through IDX for a period of 12 months. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. Cascade encourages you to remain vigilant by monitoring your accounts and reviewing the enclosed *Steps You Can Take to Help Protect Your Personal Information* for additional guidance on how to protect your personal information. There you will also find more information on the credit monitoring and identity restoration services that Perkins is offering and the steps you can take to enroll to receive them.

For More Information. Cascade understands that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call the Perkins dedicated assistance line at 1-833-933-1103, Monday through Friday, 6am to 6pm Pacific Time

Cascade sincerely regrets any inconvenience this incident may cause you and we remain committed to safeguarding your information.

Sincerely,

A handwritten signature in blue ink that reads "Kathe Hendrickson". The signature is written in a cursive, flowing style.

Kathe Hendrickson
Director – Compensation and Benefits



Steps You Can Take to Help Protect Your Personal Information

Enroll in Complimentary Credit Monitoring

1. Website and Enrollment. Perkins is offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 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. ***Please note the deadline to enroll is June 11, 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.

3. Telephone. Contact IDX at 1-833-933-1103 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity. IDX is available Monday through Friday 6am to 6pm Pacific Time.

To enroll, please call 1-833-933-1103 or visit <https://app.idx.us/account-creation/protect> and enter the activation code listed below.

Your personal IDX credit monitoring activation code is: «Enrollment_Code»

Monitor Your Accounts

We encourage you to remain vigilant against incidents of payment card fraud or misuse, to review your account statements, and to monitor your credit reports for suspicious activity. If you see any unauthorized or suspicious activity, promptly contact your bank, credit union, or credit card company.

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 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.

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

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

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

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 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 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.

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 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

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

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services



Additional Information

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, the Federal Trade Commission, or the state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); or TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **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 a 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.