Notice of Data Privacy Event

Perkins & Company, PC ("Perkins") is providing details about a cybersecurity incident that affected Netgain, a vendor Perkins uses to store data in the cloud. At this time, we remain unaware of any significant increase in suspicious activity to indicate that Perkins' client or employee information has been misused in connection with this incident and will continue to monitor this issue. We are providing individuals with details about the incident and steps individuals can take to better protect personal information, should they feel it appropriate to do so.

Who is Perkins & Co / Why Do You Have My Information? Perkins provides accounting and tax services to both individuals and organizations. As part of the services provided to organizations, Perkins handles information relating to individuals affiliated with its client businesses such as current and former employees. This cybersecurity incident occurred with Netgain, Perkins' third-party data hosting vendor. **Please know that this incident did not impact the computer systems of Perkins or its clients.**

What Happened. On December 3, 2020, Netgain alerted Perkins that Netgain 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: Between November 8, 2020, and December 3, 2020, an attacker accessed servers storing Perkins' 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 Netgain, law enforcement and the cybersecurity specialists they engaged, this attacker is not known to post the data, nor keep any copies of it once a ransom is paid. However, as there are no guarantees, Perkins considers any data viewed or stolen by the attacker to be at risk. Perkins conducted a comprehensive and time-intensive months-long programmatic and manual review of the information stored on the impacted server hosted by Netgain, to determine the types of personal information stored therein and identify the individuals to whom the personal information relates and their contact information.

What Information Was Involved. As part of the services that Perkins provides, individual's information was stored on a server that Netgain reports was accessed by the attacker, though there is no indication Perkins was intentionally targeted in this attack. The following types of personal information stored on the server hosted by Netgain which was impacted by this event varies by individual and includes name, Social Security number, date of birth, driver's license number, passport number, taxpayer identification number, financial account information, bank account information, email address and password, health insurance information, and medical information.

What Perkins is Doing. Perkins takes the security and privacy of the personal information entrusted to the company very seriously. Perkins 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. Perkins reported this incident to the IRS and state tax authorities, as well as applicable state data privacy regulatory authorities.

As an added precaution, Perkins arranged for affected individuals to enroll, at no cost, in an online credit monitoring service.

What You Can Do. Individuals can find out more about how to protect against potential identity theft and fraud in the below *Steps Individuals Can Take to Protect Personal Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions, please call our dedicated assistance line at 1-833-933-1103, available Monday through Friday, 6:00 am – 6:00 pm Pacific Time.

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. Addresses for the prior two to five years
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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. **New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. **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. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 82 Rhode Island residents impacted by this incident. **Washington D.C. Residents:** the Office of Attorney General for the District of Columbia can be reached at: 400 6th St. NW, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov. **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.