



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

OCT 07 2022

CONSUMER PROTECTION

Alexander T. Walker
Office: (267) 930-4801
Fax: (267) 930-4771
Email: awalker@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 3, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We continue to represent Perkins & Co ("Perkins") located at 1211 SW 5th Ave #1000 Portland, OR 97204, and write to supplement our August 12, 2022, notice to your office of an incident that may affect the security of certain personal information (the "August 2022 Notice"). This notice is being provided by Perkins on behalf of the data owner clients listed in ***Exhibit A***. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Perkins does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction. Perkins does not anticipate performing any additional notices to individuals or your office on behalf of itself or any other data owners.

Nature of the Data Event

As a summary of the event, on or about December 3, 2020, Netgain Technologies ("Netgain"), a vendor Perkins uses for hosting its data in the cloud, alerted Perkins to the fact that Netgain suffered a ransomware attack (the "Incident"). Upon learning of the Incident, Perkins was in regular communication with Netgain to determine the full impact of the Netgain Incident as it related to Perkins and Perkins' data as quickly as possible.

On January 15, 2021, Netgain confirmed the following: between November 8, 2020, and December 3, 2020, an unauthorized actor accessed Netgain servers that store Perkins' data, some of which the unauthorized actor copied and stole. The unauthorized actor also encrypted files and demanded a ransom payment be made by Netgain in exchange for the return of stolen files, as well as a decryption key. Netgain paid an undisclosed ransom, and the unauthorized actor returned the

Mullen.law

files they had stolen and provided Netgain with a decryption key. Per Netgain, law enforcement, and the cybersecurity specialists that Netgain engaged, the attacker group is not known to post any data, nor keep any copies of stolen data once the ransom is paid. Nevertheless, Perkins considers any data that was accessible to or acquired by the attacker to be at risk.

Upon becoming aware of the Incident, Perkins conducted its own detailed review to determine what information should be considered at risk as a result of the Netgain Incident. This included a very comprehensive and time-consuming months-long programmatic and manual review of all files contained on the impacted systems to determine the types of personal information stored therein and identify the individuals to whom the personal information relates. Perkins then conducted additional review of its internal files to confirm contact information for impacted individuals in order to provide notification of the Incident.

While the data mining was ongoing, Perkins reviewed the information that it collects and prepared a preliminary list of current Perkins employees, current individual tax clients and dependents, and corporate clients for whom Perkins handles information to perform audits of employee benefit plans. Although the data mining was still ongoing, in an abundance of caution Perkins prepared for a preliminary notification to current employees, individual tax clients, and their dependents. Perkins began notifying these individuals on March 11, 2021.

Meanwhile, on or about February 8, 2021, Perkins notified its employee benefit plan ("EBP") clients of the Netgain event and that data relating to individuals may have been impacted. These corporate EBP clients provide information for employees to Perkins for audit services. As data mining was ongoing, Perkins was not in a position to know what information specifically was impacted, but Perkins told the EBP clients that Perkins would be undertaking a data mining effort. Perkins offered to provide a notice to individuals on behalf of the EBP data owners if the data owners produced a list of individuals for whom they believed Perkins had information on the system. A number of the EBP clients opted-in to the notice offering and asked Perkins to provide notification to individuals on their behalf. Perkins provided notice to individuals and relevant state regulators on March 11, 2021, and on behalf of the EBP clients who opted-in in subsequent mailings.

At the conclusion of the data mining project, Perkins worked diligently to assess the results of the data mining in furtherance of identifying impacted individuals and notifying the Offices of the Attorneys General. Perkins mailed notice letters to individuals and notified your office on May 27, 2022, and August 12, 2022. Since the last notice, Perkins continued coordinating with the EBP data owner clients to provide the current notification to individuals and your office.

Impacted Data

Perkins confirmed that personal information relating to individuals was at risk. The impacted information may vary by individual, but includes name, Social Security number and financial account information.

Notice to New Hampshire Residents

As outlined above, on March 11, 2021, Perkins began providing written notice of this Incident to potentially affected individuals. Perkins also provided subsequent rounds of notification on behalf of Perkins and its EBP data owner clients. To date, Perkins notified three hundred seventy-nine (379) New Hampshire residents of the data event. Perkins is mailing notification to impacted individuals on behalf of additional data owners on October 3, 2022, which includes an additional seven (7) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit B*.

Other Steps Taken and To Be Taken

Upon becoming aware of the Incident, Perkins moved quickly to investigate and respond to the Incident and notify potentially affected individuals. Perkins is providing potentially impacted individuals with access to complimentary credit monitoring and identity restoration services through IDX for twelve (12) months.

Additionally, Perkins is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Perkins is providing individuals with 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4801.

Very truly yours,

Alexander T. Walker of
MULLEN COUGHLIN LLC

ATW/brb

EXHIBIT A

Data Owners

Finastra USA Corporation and Toyo Tanso USA, Inc

EXHIBIT B



Return to 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 Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

October 3, 2022

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

Perkins & Co ("Perkins") is a privately held accounting firm located in Portland, Oregon, and provides services to an organization with which you are affiliated. Perkins is writing on behalf of <<Name of Data Owner>> to provide details about a cybersecurity incident that affected Netgain, a vendor we use to store data in the cloud. At this time, we remain unaware of any significant increase in suspicious activity to indicate that Perkins' client information has been misused in connection with this incident and will continue to monitor this issue. However, because your personal information may be impacted by this incident, we are providing you with details about the incident, our 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 Do You Have My Information? Perkins provides services to <<Name of Data Owner>> and we understand you to be associated with this organization. As part of those services, Perkins handles information relating to individuals. This cybersecurity incident occurred with Netgain, Perkins' third-party data hosting vendor. **Please know that this incident did not impact the computer systems of <<Name of Data Owner>>.**

What Happened. On December 3, 2020, Netgain alerted us that they had shut down their systems and began working with outside cybersecurity specialists because of a ransomware attack on their systems that impacted our 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, we know that there are no guarantees, and we still consider any data viewed or stolen by the attacker to be at risk. Perkins conducted a comprehensive and time-intensive review of the information stored on the impacted server hosted by Netgain, and this data review process recently concluded.

What Information Was Involved. As part of the services that Perkins provides to <<Name of Data Owner>>, your 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 your personal information were stored on the server hosted by Netgain which was impacted by this event: name and <<Data Element>>.

What Perkins is Doing. Perkins takes the security and privacy of the personal information entrusted to us very seriously. 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. 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 you access to complimentary credit monitoring and identity restoration services** through IDX for a period of <<twelve(12)/twenty-four(24)>> months. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. We encourage 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 Perkins is offering and the steps you can take to enroll to receive them.

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

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

Sincerely,

Jared Holum, President
Perkins & Co

Steps You Can Take to Help Protect Your Personal Information

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: <<twelve(12)/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. Please note the deadline to enroll is January 3, 2023.

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.

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, 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. **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.