RECEIVED
AUG 15 2022
CONSUMER PROTECTION

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

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

August 12, 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 May 27, 2022, notice to your office of an incident that may affect the security of certain personal information (the "May 2022 Notice"). A copy of the May 2022 Notice is attached as ***Exhibit A*** for ease of reference. This notice is being provided on behalf of Perkins and the following data owner clients: Columbia Sportswear Company, IQ Credit Union, Mercy Corps, and Vestas American Wind Technology, Inc. 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.

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 authorized 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 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 in 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. The EBP clients who opted-in began compiling lists of individuals to whom they wanted Perkins to provide notice. 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. We previously notified your office of this incident on the following dates, while data mining was ongoing: March 11, 2021, April 23, 2021, and May 27, 2022.

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. Perkins also provided an update to its EBP data owner clients again with the offering to notify individuals and relevant regulatory authorities on their behalf. Perkins coordinated 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.

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 fifty-seven (357) New Hampshire residents of the data event. As a result of Perkins' ongoing data review efforts, Perkins continues to provide notice to affected individuals either directly or on behalf of its data owner clients. Perkins will continue mailing notification to impacted individuals on August 16, 2022, which includes an additional twenty-two (22) 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

MULLEN COUGHLIN

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

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

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

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

May 27, 2022

VIA U.S. MAIL

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

Re: 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 previous March 11, 2021, notice to your office of an incident that may affect the security of certain personal information (the "March 2021 Notice"). A copy of the initial notification is attached as **Exhibit A** for ease of reference. This notice may be supplemented with any new significant facts learned subsequent to its submission.

Nature of the Data 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 authorized actor copied and stole. The unauthorized actor also encrypted files and demanded a ransom payment be made by Netgain in exchange the return of stolen files, as well as a decryption key. Netgain paid an undisclosed ransom, and the unauthorized actor returned the 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 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 lengthy review of its internal files to confirm contact information for impacted individuals in order to provide notification of the Incident.

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

On March 11, 2021, Perkins began providing written notice of this Incident to potentially affected individuals, which included five (5) New Hampshire residents. As a result of Perkins' ongoing data review efforts, on or about May 26, 2022, Perkins continued providing notice to affected individuals which includes an additional one hundred seventy-two (172) New Hampshire residents at this time. 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/mep

EXHIBIT A

To the May 26, 2022 Submission

MULLEN COUGHLIN

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

FOREVER

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

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

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

March 11, 2021

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Perkins & Co ("Perkins") located at 1211 SW 5th Ave #1000 Portland, OR 97204, and are writing to notify your office of an incident that may affect the security of some personal information relating to five (5) New Hampshire residents. The investigation into this matter is ongoing, and this notice will 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.

Nature of the Data Event

On or about December 3, 2020, Netgain, a vendor Perkins uses for hosting its data in the cloud, alerted Perkins to the fact that Netgain suffered a ransomware attack. Upon learning of the incident, Perkins was in regular communciation with Netgain to determine the full impact of the Netgain incident as it relates 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' files, some of which the authorized actor copied and stole. The unauthorized actor also encrypted files and demanded a ransom payment be made by Netgain in exchange the return of stolen files, as well as an decryption key. Netgain paid an undisclosed ransom and the unauthorized actor returned the 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.

In addition, Perkins continues to conduct its own detailed review to determine what information should be considered at risk as a result of the Netgain event. This included a lengthy and time-consuming review of its internal records to identify the individuals whose sensitive information may have been contained in files and folders stored on Netgain's systems identified as accessible to the unauthorized actor. In addition, Perkins is working with a data mining vendor tasked with conducting a 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.

At this stage, Perkins has confirmed that personal information relating to its current and former personal tax clients and their dependents, as well as its current/former employees, is at risk. This information may vary by individual, but includes name, address, Social Security number, bank and credit card account information, insurance information, such as policy number, driver's license number, passport number, and retirement/investment account information.

As Perkins' data mining effort is still underway, it is possible Perkins may identify additional impacted individuals requiring notice in the future, and we will supplement this notice accordingly if so.

Notice to New Hampshire Residents

On March 11, 2021, Perkins began providing written notice of this incident to affected individuals, which includes five (5) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, 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 ID Experts 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, information on protecting against tax fraud, 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/mep

EXHIBIT A

To the March 11, 2021 submission

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: [XXXXXXXX]

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

March 11, 2021

Re: Notice of Data Breach

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

Perkins & Co (Perkins) is writing to provide details about the recent 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 at risk, 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.

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. As we mentioned in a prior communication, 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.

What Information Was Involved? Your Perkins client file 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. Due to your status as a current or former Perkins personal tax client or their dependent/family member, we believe the following types of personal information may have been viewed and/or stolen by the attacker: name, Social Security number, bank and credit card account information, insurance information such as policy number, drivers license number, foreign country/state identification number, passport number, and retirement and investment account information.

What Perkins is Doing. Perkins takes the security and privacy of the personal information entrusted to us very seriously. In addition to our actions addressed above, we have partnered with an outside data mining vendor to determine precisely what and whose personal information may have been impacted by this incident. 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 your minor dependent access to complimentary credit monitoring and identity restoration services** through IDX for a period of <<12 months/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 reviewing the enclosed *Steps You Can Take to Help Protect Your Personal Information* for additional guidance on how to protect your minor dependent's personal information. There you will also find more information on the credit monitoring and identity restoration services Perkins is offering and the steps your minor dependent 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, 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: <<12 months/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 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.

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	**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

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 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 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	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

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 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. **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 <<Number of RI Resident>> 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.

EXHIBIT B

To the May 26, 2022 Submission

PERKINS & CO
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>>

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

May 25, 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 accounting and tax services to both individuals and organizations. Perkins is writing 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 or employee 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 event, 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 accounting and tax services to both individuals and organizations. 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 Perkins or its clients.**

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. As we mentioned in a prior communication, 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, 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 <<Variable Text - data elements>>.

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 August 26, 2022.

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. **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.

EXHIBIT B

Perkins & Co

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>>

August 16, 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 <<Variable Text – 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 at risk, 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 <<Variable Text – 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 <<Variable Text – 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 **<<Variable Text – 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 was stored on the server hosted by Netgain which was impacted by this event: name, and <<Data Elements>>.

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 November 16, 2022.

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. **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 14 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.

2022 AUG 15 PM 1:09
DEPT OF JUSTICE
STATE OF NH