<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<First_Name>> <<Last_Name>>,

As a current employee of Dietzgen Corporation d/b/a Sihl, Inc. ("Sihl"), we value and respect the privacy of your information, which is why we are writing regarding a recent security incident involving some of your personal information. This letter contains information about what happened, the measures taken in response, and steps you can take to help protect your information.

WHAT HAPPENED?

We recently detected a security event impacting our internal systems and took immediate steps to investigate, contain, and eradicate the incident with the assistance of outside forensic consultants. The investigation determined that an unauthorized third party accessed and copied files contained within certain segments of our network between August 26, 2024 and August 27, 2024. Upon making this determination, we initiated a detailed review of these files to determine whether individuals' personal information was accessed by the unauthorized party. That review concluded on December 5, 2024; at which time we determined that some of your personal information was contained within the affected files.

We are aware that a limited number of files copied by the unauthorized party were briefly published online. However, we promptly addressed this situation, ensuring that the published files were taken down and subsequently deleted. While certain files were published online, they were only available for a short period, and we confirmed that the files were viewed only by parties authorized by us, including the cybersecurity professionals assisting us in responding to this incident. As of now, we have no evidence that your personal information was accessed by any additional unauthorized parties, nor do we have any reason to believe that your personal information has been or will be used inappropriately or without authorization.

WHAT INFORMATION WAS INVOLVED?

We are notifying you out of an abundance of caution because information related to you was identified in the files that the threat actor potentially accessed. The records included some of your personal information, including your full name and possibly, in a few instances, your date of birth, Social Security number, driver's license number, bank account and routing number, and/or health insurance information (if such information was shared with us as part of your employment with Sihl).

WHAT WE ARE DOING.

In response to this incident, we took immediate steps to contain and secure our network. Specifically, we restricted access to the affected servers and accounts to prevent further unauthorized access. We have also hired a cybersecurity consulting firm to assist us in remediating the incident and to help us enhance existing security protocols across our network so we can effectively monitor for suspicious activity and protect your personal information. We have also notified federal law enforcement authorities of the incident.

Additionally, we acted promptly to mitigate potential risks associated with the brief online publication of a limited number of files, including ensuring that the published files were taken down and subsequently deleted. We continue to work with our cybersecurity professionals to protect your personal information.

Though we have no evidence that your personal information was widely exposed or has been used inappropriately or without authorization, we also have arranged for you to activate, at no cost to you, a comprehensive identity monitoring service for <<ServiceTerminMonths>> months provided by Kroll. A description of this service and instructions on how to activate can be found below in the "Other Important Information" document included with this letter. Please note that you must activate to take advantage of this free service, and we encourage you to do so.

WHAT YOU CAN DO.

If you have not already done so, you can activate your identity monitoring services by following the instructions in the section below titled Identity Monitoring. Please review the enclosed "Other Important Information" document included with this letter for further steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It is also recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, you should promptly notify the financial institution or company with which your account is maintained.

IDENTITY MONITORING.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **<<b2b_text_6 (ActivationDeadline)>>** to activate your identity monitoring services.*

Membership Number: **<<Membership Number (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

FOR MORE INFORMATION.

For further information and assistance, please contact our dedicated incident response line at TFN, between 9:00 a.m. – 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Chris Cudzilo
Managing Director
Sihl, Inc.

OTHER IMPORTANT INFORMATION

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Innovis, PO Box 1689, Pittsburgh, PA 15230-1689, www.innovis.com, 1-800-540-2505

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For 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/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.