Unity Technologies SF
c/o Equifax Inc
116 New Montgomery St, Suite 300
San Francisco, CA 94105

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

Notice of Data Breach

Dear <<Full Name>>,

Thank you for being a valued customer of Unity Technologies. We are writing to inform you about a recent security incident involving the SpeedTree website operated by Unity Technologies. This incident may have affected your information entered during the checkout process if you made a purchase on through the SpeedTree website between March 13, 2025, and August 26, 2025.

We encourage you to read this letter carefully as it contains important information regarding the incident, our response, and steps you can take to help protect your information.

What Happened?
On August 26, 2025, we became aware of a security incident involving the SpeedTree website operated by Unity Technologies. Upon discovery, we promptly disabled the site and initiated an investigation with the support of external cybersecurity specialists. Our investigation determined that the incident involved an unauthorized code that had been added to the check-out page of the SpeedTree website around March 13, 2025. We promptly removed this code upon its discovery on August 26, 2025. This unauthorized code potentially allowed an unauthorized individual to capture information entered during the checkout process on the SpeedTree product page.

What Information Was Involved?
Individuals who made purchases on the SpeedTree website between March 13, 2025, and August 26, 2025, may have been impacted. Upon reviewing our records, we identified that you may have made a purchase during the timeframe when the unauthorized code was active. Accordingly, the information you entered at SpeedTree's checkout page — such as your name, address, email address, credit card number, and access code — may have been affected.

What Are We Doing?
We take this situation seriously, and we apologize for any inconvenience or concern this incident may cause. Upon becoming aware of the suspicious activity, we moved immediately to investigate and respond. The investigation actions included steps to assess and secure our network and continue our normal business operations, review the relevant involved files, notify potentially involved clients and associated individuals, and notify the appropriate data protection authorities, as applicable.

We are also offering you complimentary credit monitoring and identity protection services for 12-months to help you safeguard your information. Additionally, we are providing further information on steps you can take to help

protect your information. More details about these complimentary services can be found in the next section as well as in the attached Equifax Credit Watch™ Gold instructions page.

What You Can Do.
We strongly recommend reviewing the steps outlined below to safeguard your information and enrolling in the complimentary credit monitoring and identity protection services we offer. Cybersecurity is an ongoing concern for everyone, as companies worldwide face increasing threats. By following the steps provided, individuals can better protect themselves.

1. **Enroll in Complimentary Credit Monitoring and Identity Protection Services.** We have arranged for Equifax to provide you with 12 months of complimentary credit monitoring and identity protection services through Equifax Credit Watch™ Gold. Please refer to the attached Equifax Credit Watch™ Gold information page for details on:

    - Key benefits of the service
    - Enrollment instructions
    - Enrollment deadline
        - *Note: You must complete enrollment before the deadline listed in the attachment to activate your complimentary services.*
    - Other important information

2. **Review Your Accounts for Suspicious Activity.** We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity. If you entered your card information on the SpeedTree site between March 13, 2025, and August 26, 2025, you might want to consider contacting your issuing bank to discuss the option of obtaining a new card with a different account number as a precautionary measure.

3. **Order A Credit Report.** To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

    Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

    If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

4. **Contact the Federal Trade Commission, State Attorney General, or Law Enforcement Authorities**. You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to the FTC, your state Attorney General's office, or law enforcement authorities. Please note, this notification was not delayed by law enforcement authorities.

To learn more about how to protect yourself from becoming a victim of identity theft, you can contact the FTC at: The Federal Trade Commission**,** Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-FTC-HELP (1-877-382-4357) (toll-free) or 1-877-IDTHEFT (1-877-438-4338); and www.identitytheft.gov and www.ftc.gov/idtheft/.

5. **Additional Rights Under the Fair Credit Reporting Act**. You have rights pursuant to the Fair Credit Reporting Act ("FCRA"), 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 FCRA, 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 violators. You may have additional rights under the FCRA not summarized here.

   Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf or writing to the Consumer Financial Protection Bureau at: Consumer Financial Protection Bureau, 1700 G Street, NW, Washington, DC 20552.

6. **Place a Fraud Alert on Your Credit File**. You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. You may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

Equifax	Experian	TransUnion
P.O. Box 105069 Atlanta, Georgia 30348 1-800-525-6285 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	P.O. Box 9554 Allen, Texas 75013 1-888-397-3742 https://www.experian.com/help/fraud-alert/	P.O. Box 2000 Chester, Pennsylvania 19016 1-800-916-8800 https://www.transunion.com/fraud-alerts

7. **Request Security Freezes.** You have the right to request a security freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

   Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity.

   The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide the following information:

   - Your full name, with middle initial as well as Jr., Sr., II, etc.
   - Social Security number
   - Date of birth

- Current address and all addresses for the past five years
- Proof of current address, such as a current utility bill or telephone bill
- Social Security Card, pay stub, or W-2;
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, military identification, or birth certificate; and/or
- Any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles if you are a victim of identity theft

Below, please find the relevant contact information for the three consumer reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, Georgia 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, Texas 75013 1-888-397-3742 https://www.experian.com/help/credit-freeze/	P.O. Box 160 Woodlyn, Pennsylvania 19094 1-800-916-8800 https://www.transunion.com/credit-freeze

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than 5 business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future. Each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Other Important Information.

1. **For Iowa Residents**. You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft at: Consumer Protection Division, Security Breach Notifications, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319; 1-515-281-5164 or 1-888-777-4590 (toll-free); and www.iowaattorneygeneral.gov.

2. **For Maryland Residents**. You can obtain information about avoiding identity theft from the Maryland Attorney General or the FTC. Contact information for the FTC is included above. The Maryland Attorney General can be contacted at: Office of the Maryland Attorney, General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023 (toll-free); and www.marylandattorneygeneral.gov.

3. **For Massachusetts Residents**. You have the right to obtain a police report and request a security freeze (without any charge) as described above.

4. **For New York Residents**. You can obtain information about security breach response and identity theft prevention and protection from the New York Attorney General at: New York Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755 or 1-800-788-9898 (toll-free); and https://ag.ny.gov/.

5. **For New Mexico Residents**. You can review your personal account statements and credit reports to detect errors resulting from this matter by utilizing the resources provided above. As a consumer, you also have certain rights pursuant to the FCRA as described above.

6. **For North Carolina Residents**. You can obtain information about avoiding identity theft from the North Carolina Attorney General or the FTC. Contact information for the FTC is included above. The North Carolina Attorney General can be contacted at: Office of the North Carolina Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; 1-919-716-6400 or 1-877-566-7226 (toll-free); and https://www.ncdoj.gov/.

7. **For Oregon Residents**. You may report suspected identity theft to law enforcement, including the Office of the Oregon Attorney General or the FTC. Contact information for the FTC is included above. The Oregon Attorney General can be contacted at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; and https://www.doj.state.or.us/.

8. **For Rhode Island Residents**. You have the right to obtain a police report and request a security freeze (without any charge) as described above. The Rhode Island Office of the Attorney General can be contacted at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and https://riag.ri.gov/.http://www.riag.ri.gov/ Information pertaining to approximately two Rhode Island residents was potentially involved in this incident.

9. **For Washington, DC Residents**. You have the right to request a security freeze (without any charge) as described above. You can obtain information about avoiding identity theft from the District of Columbia Attorney General or the FTC. Contact information for the FTC is included above. The District of Columbia Attorney General can be contacted at: The District of Columbia Attorney General, 400 6th Street NW, Washington, DC 20001; 1-202-727-3400; and www.oag.dc.gov.

For More Information.

We understand that this situation might raise questions or concerns, and we are here to support you. If you have any inquiries that were not addressed in this letter, please feel free to reach out to us. You can contact us via email at DPO@unity3d.com, write to us at 116 New Montgomery St, San Francisco, CA 94105, or call us at +1 (209) 442-7024.

As mentioned earlier, if you need assistance with enrollment or have questions about the complimentary Equifax Credit Watch™ Gold services, please contact Equifax directly using the information provided in this letter. Protecting the data entrusted to us remains our top priority, and we sincerely regret any inconvenience or concern this may cause you.

Once again, thank you for being a valued Unity Technologies customer. We sincerely apologize for this incident and stand ready to assist you in any way we can.

Sincerely,

Jamie Crabtree, Data Protection Officer
Unity Technologies