EXHIBIT 1

We continue to represent Stride Inc. ("Stride"), located at 2300 Corporate Park Drive, Herndon, VA 20171, and write to supplement the notice provided to your Office on June 11, 2021. Our previous submission is attached here as ***Exhibit AA***.

Based on ongoing efforts to reconcile data and determine contact information for individuals, on July 6, 2021, Stride will provide notice to an additional thirteen (13) Maine residents. The affected personal information as defined by Me. Rev. Stat. Ann. tit. 10 § 1347(6) that was identified in relation to Maine residents includes name and Social Security number. Written notice is being provided in substantially the same form as the letter attached to our June 11, 2021 submission to your Office.

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Stride does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

EXHIBIT AA

Maine Security Breach Reporting Form

Thank you for submitting the breach details through this reporting form. The information you have provided has been submitted to the agency.

Please close this browser window.

PREVIOUS FINISH

Maine Security Breach Reporting Form

Pursuant to the Notice of Risk to Personal Data Act (Maine Revised Statutes 10 M.R.S.A. §§1346-1350-B)

Entity that owns or maintains the computerized data that was subject to the breach:

Type of Organization (Please select one) *

Education

Entity Name *

Stride, Inc.

Street Address *

2300 Corporate Park Drive

City *

Herndon

State, or Country if outside the US *

VA

Zip Code *

20171

Submitted by:

Name *

Vincent Mathis

Title *

Executive Vice President, General Counsel & Secretary

Firm name (if different than entity name)

Telephone Number *

(703) 483-7482

Email Address *

vmathis@k12.com

Relationship to entity whose information was compromised *

General Counsel

Breach Information:

Total number of persons affected (including Maine residents) *

13740

Total number of Maine residents affected *

26

If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified?

Please select an option

Date(s) Breach Occurred *

11/04/20 – 11/19/20

Date Format: mm/dd/yyyy

Date Breach Discovered *

05/19/221

Description of the Breach (please check all that apply)

- [ ] Loss or theft of device or media (computer, laptop, external hard drive, thumb drive, CD, tape, etc.)
- [ ] Internal system breach
- [ ] Insider wrongdoing
- [x] External system breach (hacking)
- [ ] Inadvertent disclosure
- [ ] Other

If other, please specify

Information Acquired - Name or other personal identifier in combination with (please check all that apply)

- [x] Social Security Number
- [ ] Driver's License Number or Non-Driver Identification Card Number

☐ Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account)

Notification and Protection Services:

Type of notification *

Written

Date(s) of consumer notification *

06/11/21

Date Format: mm/dd/yyyy

Please attach a copy of the template of the notice to affected Maine residents

FILE

Uploaded Files:

Stride - Notice of Data Event - ME.pdf Delete

List dates of any previous (within 12 months) breach notifications

Were identity theft protection services offered? *

Yes

If yes, please provide the duration, the provider of the service and a brief description of the service

12 months. Experian, credit monitoring and identity protection

CONTINUE TO REVIEW >

EXHIBIT 1

By providing this notice, Stride does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around November 11, 2020, Stride was the victim of a ransomware attack. Upon discovering an incident impacting certain portions of its network, Stride quickly took steps to lock down affected systems, notified federal law enforcement authorities, and began working with a third-party forensics team to investigate and assist with the incident. Working with third-party forensic investigators, Stride determined that an unknown actor may have gained access to Stride systems from November 4, 2020 to November 19, 2020.

Once the incident was contained, Stride initiated a comprehensive review, with the assistance of industry-leading forensic specialists, to identify any information of individuals contained in the files affected by the incident. That third-party review, which involved a complex and large data set, was completed in April 2021. Stride then undertook a comprehensive internal reconciliation of the records found to identify individuals and confirm contact information. While this effort is still on going, on or around May 19, 2021, Stride confirmed that the affected data includes information related to Maine residents. The affected personal information as defined by Me. Rev. Stat. Ann. tit. 10 § 1347(6) that was identified in relation to Maine residents includes name and Social Security number.

Notice to Maine Residents

On June 11, 2021, Stride will begin mailing written notice of this incident to affected individuals, including approximately twenty-six (26) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A.***

Other Steps Taken and To Be Taken

Upon discovering the event, Stride moved quickly to investigate and respond to the incident, assess the security of Stride systems, and review the affected data to identify impacted individuals. Stride also Stride worked extensively with an industry-leading third-party forensics firm to ensure that we are taking all appropriate steps to prevent any incident like this from happening again, including identifying and removing all infected machines from the network. Stride is also undertaking a top-to-bottom review of its security posture, working with outside security experts to ensure that it is taking all appropriate steps to protect its systems and to continue to reduce the risk of future incidents.

Additionally, Stride is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. Stride is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

EXHIBIT A

Stride

Return Mail Processing
PO Box 999
Suwanee, GA 30024

June 11, 2021

59 1 13603 **********AUTO**ALL FOR AADC 800
SAMPLE A. SAMPLE - L03
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Re: [Extra1]

Dear Sample A. Sample:

Stride Inc. ("Stride") writes to let you know about a data security incident that we discovered that affected some of your information. Because the security of our employees' information is of utmost importance to us, we are notifying you of the event as well as resources available to you to help protect your information, should you feel it necessary to do so.

What Happened? On or around November 11, 2020, Stride was the victim of a ransomware attack. Ransomware is a form of attack in which, after gaining access to a system, the attacker encrypts a victim's files and then demands a ransom to restore access to the data. Educational institutions, from primary schools through higher education, are increasingly becoming a target of ransomware attacks.

As soon as we discovered that our systems had been infected with ransomware, we quickly took steps to lock down impacted systems, notified federal law enforcement authorities, and began working with an industry-leading third-party forensics team to investigate and assist with the incident. Working with third-party forensic investigators, Stride determined that an unknown actor may have gained access to Stride systems from November 4, 2020 to November 19, 2020.

After careful consideration, we also decided to make a payment to the ransomware attacker, as a proactive and preventive step in exchange for assurance that the information obtained by the attacker from our systems would be returned to Stride and would not be released on the Internet or otherwise disclosed. While there is always a risk that the threat actor will not adhere to negotiated terms, based on guidance we have received about the attack and the threat actor, the company believes the payment was a reasonable measure to take in order to prevent misuse of any information the attacker obtained.

Once the incident was contained, Stride initiated a comprehensive review, with the assistance of industry-leading forensic specialists, to identify any information of individuals contained in the files affected by the incident. Stride also then undertook a comprehensive internal effort to reconcile the results of the third-party review and find contact information for the affected individuals. [Extra4] As soon as Stride was aware that our employees' information was impacted, including yours, we worked as quickly as possible to notify you.

As you may already be aware, going forward, as part of our ongoing commitment to the security of information we are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

What Information is Involved? Our review determined that the affected data contained your name and [Extra2].

What Are We Doing? As mentioned previously, we take this incident and the security of our employees' information in our care seriously. Importantly, we have no indication that any of the data affected in the incident has been or will be misused. Following the payment we made to the attacker, the attacker returned the data they claimed to have obtained from Stride's systems. Stride subsequently engaged an industry-leading third-party specialist to conduct a search for the data on the Internet (including the "dark web") and found no evidence of data related to this incident being published, posted for sale, or otherwise disclosed.

What You Can Do. As a matter of general practice, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information.*

As an added precaution, we are offering you access to complimentary credit monitoring and identity protection services for [Extra3] months through Experian. These services include fraud consultation and identity theft restoration services. If you wish to activate the credit monitoring and identity protection services, you may follow the instructions included in the *Steps You Can Take to Help Protect Your Information*.

For More Information. If you have any additional questions, please call the assistance line we have set up for this matter at (855) 414-6049 from Monday to Friday 6:00am – 8:00pm PST and Saturday to Sunday 8:00am – 5:00pm PST by August 31, 2021.

Sincerely,

Valerie Maddy
Senior Vice President - Human Resources
Stride Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

What we are doing to protect your information:
To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **08/31/2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (855) 414-6049 by **08/31/2021.** Be prepared to provide engagement number **B013662** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Monitor Your Accounts

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

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 with the credit reporting bureau. 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, 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
1-888-298-0045	1-888-397-3742	1-833-395-6938
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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St NW, Washington, DC 20001, United States; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Stride Inc. is located at 2300 Corporate Park Drive Herndon, VA 20171.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 19 Rhode Island residents impacted by this incident.

For 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 bureaus 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 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. We encourage you to 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.