Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

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

July 28, 2020

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notification
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Front Rush, LLC ("Front Rush"), located at 1333 N. Kingsbury Street, FL 4, Chicago IL, 60642. Front Rush maintains data on behalf of certain data owners and is writing to notify your office, on its own behalf and their behalf, of an incident that may affect the privacy of personal information relating to seven hundred and thirty-five (735) Iowa residents. Front Rush reserves the right to supplement this notice with new significant facts learned subsequent to its submission. By providing this notice, Front Rush does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

Front Rush provides athletics management software solutions to academic institutions and amateur athletics organizations ("institutions"). On January 5, 2020, Front Rush was informed by a security researcher that one of its Amazon Web Services S3 buckets ("the S3 bucket") was publicly accessible from the internet. The S3 bucket contained: (a) certain attachments (like transcripts, injury reports, or athletic reports) that were placed in the platform by the institutions; and (b) certain attachments that were uploaded by student-athletes, prospective student-athletes or their parents/guardians, in response to prompts in a recruitment questionnaire formulated and disseminated by the institutions.

Upon learning of this event, Front Rush immediately commenced an investigation, working with third-party forensic investigators, to assess the nature and scope of the incident. The investigation determined that the S3 bucket was likely publicly accessible between January 18, 2016 and January 8, 2020. The investigation also determined that Front Rush's own internal database and systems were unaffected by this incident. Front Rush also contacted the security researcher, who stated that he did not save or share any copies of the data. Although Front Rush has no evidence to suggest that the S3 bucket was accessed by anyone other than the security researcher, logs were not sufficient to show whether anyone else had accessed the data. Out of an abundance of caution, Front Rush undertook a comprehensive programmatic and manual review of the entire contents of the S3 bucket to confirm the type of information contained in the S3 bucket and the individuals to whom it related.

On January 10, 2020, Front Rush began notifying affected institutions that information relating to individuals may have been affected by this incident, based on information it had available at that time. Once Front Rush completed the comprehensive review of the entire contents of the S3 bucket to confirm the type of information contained in the bucket and the individuals to whom it related, Front Rush notified the affected institutions, offered to provide notification services, and worked with institutions to confirm the contact information for these individuals. These notifications were sent to the institutions on June 15, 2020. Front Rush offered the institutions the opportunity to opt out of notices and to provide supplemental or additional address information.

The investigation determined that the following types of information related to Iowa residents was accessible within the S3 bucket: Social Security number and other identification number. To date, the investigation has found no evidence of any actual or attempted misuse of personal information as a result of this event.

Notice to Iowa Residents

On or around July 27, 2020, Front Rush began providing written notice of this incident to potentially affected individuals. This includes approximately seven hundred and thirty-five (735) Iowa residents whose personal information under Iowa law may have been accessible. Written notice to the individuals is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of this event Front Rush immediately commenced an investigation, working with third-party forensic investigators, to assess the nature and scope of the incident, as well as what data may potentially be affected. Front Rush provided notice to data owner institutions that had associated-individuals' data potentially accessible through the publicly accessible S3 bucket. Front Rush is also offering complimentary access to twelve (12) months of credit and identity monitoring services, including identity restoration services, through TransUnion or Equifax for individuals whose Social Security number or driver's license was potentially exposed, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident.

Additionally, Front Rush is providing affected individuals with guidance on how to better protect against identity theft and fraud. This guidance includes 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 about incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, the respective state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Front Rush will also be providing notice of this event to other regulators as may be required under applicable state law.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF:hyb
Enclosure

Exhibit A

FRONT RUSH™

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Front Rush, LLC ("Front Rush") is writing to notify you on behalf of itself and its customers about an incident that may affect the privacy of some of your personal information. Front Rush provides athletics management software solutions to academic institutions and amateur athletics organizations ("institutions"). One or several of these institutions recruited you as a student athlete, or you may have been a member of one or more institutions, and some of your information was stored within Front Rush's systems due to the institutions' use of Front Rush. While we are unaware of any actual or attempted misuse of your information, this letter provides details of the incident, our response, and resources available to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or around January 5, 2020, Front Rush was informed by a security researcher that one of its Amazon Web Services S3 buckets ("the S3 bucket") was publicly accessible from the internet. The S3 bucket contained: (a) certain attachments (like transcripts, injury reports, or athletic reports) that were placed in the platform by the institutions; and (b) certain attachments that were uploaded by student-athletes, prospective student-athletes or their parents/guardians, in response to prompts in a recruitment questionnaire formulated and disseminated by the institutions.

Upon learning of this event, we immediately commenced an investigation, working with third-party forensic investigators, to assess the nature and scope of the incident. The investigation determined that the S3 bucket was publicly accessible between January 18, 2016 and January 8, 2020. Front Rush's own internal database and systems were not affected by this incident. We also contacted the security researcher, who stated that he did not save or share any copies of the data. Although we have no evidence to suggest that the S3 bucket was accessed by anyone other than the security researcher, logs were not sufficient to show whether anyone else had accessed the data. Out of an abundance of caution, we undertook a comprehensive programmatic and manual review of the entire contents of the S3 bucket to confirm the type of information contained in the S3 bucket and the individuals to whom it related. We received results of the data mining investigation on May 19, 2020 and began parsing the data to notify impacted institutions. The institutions were notified that your information was confirmed to be impacted on June 15, 2020.

What Information Was Involved? Although we do not have any evidence demonstrating that your information was accessed or acquired, our investigation determined the information present in the S3 bucket included your name and the following types of personal information: <<Breached Elements>>.

What Are We Doing? We take this incident and the security of your personal information seriously. Upon learning of this incident, Front Rush immediately took steps to reconfigure and secure the S3 bucket to ensure it was no longer publicly accessible, and launched an in-depth investigation to determine the nature and scope of the incident. Front Rush also notified its customer institutions and updated them as the investigation unfolded. As part of Front Rush's ongoing commitment to the privacy of personal information in its care, Front Rush also reviewed its existing policies and procedures to ensure the security of information in its systems. Front Rush will continue working to further secure the information in its systems going forward. Front Rush is also notifying state regulatory authorities, where required.

As an added precaution, Front Rush is also offering you complimentary access to <<CM Length>> months of identity monitoring, fraud consultation and identity theft restoration services through TransUnion. If you wish to activate these services, you may follow the instructions included in the "Steps You Can Take to Protect Your Information."

What Can You Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Additionally, please review the enclosed "Steps You Can Take to Protect Your Information." You may also enroll to receive the credit monitoring and identity theft protection services we are making available to you. Front Rush is making these services available at no cost to you; however, you will need to enroll yourself in these services.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-917-3546 (toll free), Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Time (excluding U.S. national holidays).

We sincerely regret any inconvenience this incident may cause you. Protecting your information is important to us, and Front Rush remains committed to safeguarding information in our care.

Sincerely,

Mike Thrower
General Manager
Front Rush

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring and Identity Theft Protection Services

Visit **www.MyTrueIdentity.com** to activate and take advantage of these services.
You have until **<<Enrollment Deadline>>** *to activate these services.*
Your Activation Code is: **<<Insert Activation Code>>**

To enroll in this service, go to the *my*TrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, promptly change any involved account passwords, and to review account statements, and credit reports for suspicious activity. Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) 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 (3) major credit bureaus directly to request a free copy of your credit report. You may wish to stagger your requests so that you receive a free report by one of the three (3) credit bureaus every four (4) months.

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

In order 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 lived over the prior five (5) 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. 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.

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

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	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-alerts	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 your 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); 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 North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or https://www.marylandattorneygeneral.gov/.

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 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 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 to Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; or 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 approximately 64 Rhode Island residents whose personal information was present in the S3 bucket.