

EXHIBIT A



One Financial Center
Boston, MA 02111

August 4, 2022

NOTICE OF DATA BREACH

Dear _____ :

Brown Rudnick LLP (“Brown Rudnick” or “we”) is writing to notify you of a recent data incident that may involve some of your information. At this time, we have no evidence that your information has been or will be misused. Out of an abundance of caution, we are providing you with information about the event, our response to it, and resources available to help protect your information, should you feel it appropriate to do so.

What Happened? On May 18, 2022, we became aware of unusual activity in an employee’s e-mail account. In response, we immediately took steps to secure the e-mail account and began working with third-party incident response and data forensic specialists to investigate the nature and scope of the incident. Through the investigation, we determined that there was a brief period of unauthorized access by an unknown individual (or individuals) to two company Microsoft 365 online e-mail accounts between May 17, 2022 to May 18, 2022 for one account, and only on May 26, 2022 for the second account. However, the investigation was unable to determine whether any specific emails within the accounts were actually accessed or viewed. We then worked diligently to review the e-mail accounts to determine whether sensitive information may have been contained within the accessed e-mail accounts and identify the individuals whose information may have been impacted. Through this review, we determined that some of your information was present in the impacted e-mail account(s). This review is ongoing at this time, but on July 5, 2022, we determined some information pertaining to you may have been impacted.

What Information Was Involved? We are notifying you out of an abundance of caution because the investigation determined that certain information relating to you may have been included in the impacted files. The potentially impacted information may include _____ At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. We take this incident and security of your information seriously. Upon discovering this incident, we immediately took steps to review and then remediate the circumstances that led to the incident. We will continue our standard practice of reviewing our security policies, procedures, and processes, to ensure our measures adhere to industry best practices and reduce the likelihood of a similar future incident. We will also notify applicable regulatory authorities, as required by law.

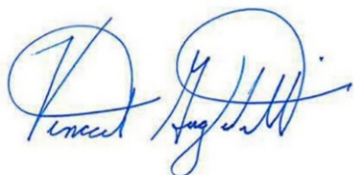
As an added precaution, we are also offering 12 months of complimentary access to credit monitoring services through Epiq. Individuals who wish to receive these services must enroll by following the enrollment instructions found in the enclosed *Steps You Can Take to Help Protect Your Information*.

What You Can Do. 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 over the next 12 to 24 months. You can find out more about how to protect your information in the enclosed *Steps You*

Can Take to Help Protect Your Information. There you will also find more information on the credit monitoring services we are offering and how to enroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call us at 1.617.856.8522.

Sincerely,

A handwritten signature in blue ink, appearing to read "Vincent J. Guglielmotti". The signature is stylized with large, overlapping loops and a long horizontal stroke extending to the right.

Vincent J. Guglielmotti
Partner, CEO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, 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 following 6-digit telephone pass code **699881** 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.

You can sign up for the online or offline credit monitoring service anytime between now and **November 30, 2022**. Due to privacy laws, we cannot register you directly. 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, or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

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.

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.);
1. Social Security number;
2. Date of birth;
3. Addresses for the prior two to five years;
4. Proof of current address, such as a current utility bill or telephone bill;
5. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
6. 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 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.

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

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/>.

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.

EXHIBIT B

brownrudnick

STATEMENT

For Immediate Release:

LOS ANGELES, CALIFORNIA– NOTICE OF DATA EVENT

Los Angeles, CA, August 26, 2022 – Brown Rudnick LLP (“Firm” or “we”) is providing notice of a recent data privacy incident that may have resulted in unauthorized access to certain information. The following notice includes information about the event, steps taken since discovering the event, and resources available to help individuals protect against potential misuse of their information, should they feel it is appropriate to do so. *At this time, we have no indication that any information was subject to actual or attempted misuse as a result of this incident.*

What Happened? On May 18, 2022, we became aware of unusual activity in an employee’s online e-mail account. We immediately took steps to secure the e-mail account and began working with experienced incident response and data forensic specialists to investigate the nature and scope of the incident. Through the investigation, we determined that there was a brief period of unauthorized access to two Firm Microsoft 365 online e-mail accounts between May 17-18, 2022, for one account, and on May 26, 2022, for the second account. The investigation was unable to determine whether any specific e-mails within the accounts were accessed or viewed. We then worked diligently to review the e-mail accounts to determine whether sensitive information may have been contained within the accessed e-mail accounts and to identify the individuals whose information may have been impacted.

What Information Was Involved? On July 5, 2022, we determined the information at issue, which potentially includes a person’s name, Social Security number, and medical information. Not all information was present for each individual. On August 4, 2022, we started sending notification letters to impacted individuals for whom we had addresses. Ordinarily, if you were or are a client of the Firm, and we determined that you may have been affected by this incident, we would have sent a notification letter to you at your last known address.

What We Are Doing. Upon discovering this incident, we immediately took steps to review and then remediate the circumstances that led to the incident. We will continue our standard practice of reviewing our security policies, procedures, and processes, to ensure our measures adhere to industry best practices and reduce the likelihood of a similar future incident. We also notified applicable regulatory authorities, as required by law.

What You Can Do. We encourage potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms for suspicious activity. The Firm is providing potentially impacted individuals with contact information for the three major credit reporting agencies, as well as providing advice on how to obtain free credit reports and how to place fraud alerts and security freezes on their credit files. The relevant contact information is 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
--	---	--

Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their 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.

For More Information. If you believe you may have had personal data exposed by this event and you have additional questions that are not addressed here, please call our dedicated assistance line at 1.617.856.8522. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.