EXHIBIT A

Jud Welle
Partner
+1 212 459 7400
JWelle@goodwinlaw.com

Goodwin Procter LLP
The New York Times Building
620 Eighth Avenue
New York, New York 10018

goodwinlaw.com
+1 212 813 8800

CONFIDENTIAL TREATMENT REQUESTED

October 17, 2024

RE: Notice of Data Event

Dear Sir or Madam:

We represent Loring, Wolcott & Coolidge ("LWC") and are writing to notify your Office of a compromise that affected the security of certain personal information relating to 2,390 Massachusetts residents. LWC offers a wide range of fiduciary and investment management services. By providing this notice, LWC does not waive any rights or defenses, including but not limited to rights or defenses regarding the applicability of Massachusetts law, the applicability of Massachusetts data event notification statute, or personal jurisdiction.

Notice of Data Event

On May 12, 2024, LWC discovered suspicious activity within its environment (the "Incident"). LWC initiated its incident response protocols and promptly began an investigation with the assistance of third-party cybersecurity specialists, retained through outside counsel, to determine the nature and scope of the suspicious activity. Additionally, in conjunction with the forensic investigation, LWC also worked to contain and remediate the Incident, an effort which has since been completed. As part of its response to this Incident, LWC took steps to implement additional safeguards to further protect the security of its systems. Additionally, LWC notified and consulted with law enforcement throughout the course of the Incident.

The in-depth cyber forensic investigation determined that unauthorized activity occurred between April 26, 2024 and May 12, 2024, that LWC's systems were impacted by malware, and that a certain amount of data was subject to unauthorized access and in some cases acquisition. With the assistance of a third-party data analytics firm, also retained through outside counsel, LWC conducted a comprehensive and time-intensive review of the data at issue to determine the types of personal information at risk and identify to whom the personal information relates. In addition, LWC conducted a review of its internal files to further assess the impacted data. Following the review, LWC determined that personal information relating to Massachusetts residents was subject to unauthorized access/acquisition.

The information impacted varies by individual but includes some or all of the following: name, address, Social Security number, driver's license number or state ID number, passport number, bank account number, username and password or email address and password, Tax Identification Number (TIN), IRS PIN, debit/credit card number, health/medical insurance policy number, mother's maiden name.

Notice to Massachusetts Residents

On October 17, 2024, LWC began providing written notice of the Incident to potentially impacted individuals, on a rolling basis, which includes Massachusetts residents. Written notice is being provided in substantially the same

form as the letter attached hereto as *Exhibit A.* Please also note that LWC is also providing substitute notice of the Incident.

Other Steps Taken and to be Taken

Upon discovery of the Incident, LWC moved quickly to investigate and respond to the Incident, assess the security of its systems, and notify potentially impacted individuals. LWC also reviewed its existing policies and procedures and implemented additional safeguards to further secure its systems and the information contained therein.

Although LWC is unaware of any instances since the Incident occurred in which the personal information has been fraudulently used, LWC is nevertheless offering potentially impacted individuals with access to complimentary credit monitoring for three (3) years and dedicated call center services as well as providing guidance on how to protect against identity theft and fraud, including advising individuals to report any suspected identity theft or fraud to their financial institutions. LWC is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national credit reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the Incident, please contact me at (212) 459 7400 or cyber@goodwinlaw.com

Respectfully submitted,

Goodwin Procter LLP

/s/ Jud Welle

Jud Welle
Partner

JW

EXHIBIT 1

LWC
LORING, WOLCOTT & COOLIDGE
Trusted Relationships for Generations

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>><<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

October 17, 2024

Re: Notice of Security Incident

Dear <<First Name>><<Last Name>>:

Loring, Wolcott & Coolidge ("LWC") is writing to advise you of a recent event that may impact the security of certain personal information related to you. We write to provide you with the steps we have taken since discovering the incident, and the steps you can take to better protect your information should you feel it appropriate to do so.

Between April 26, 2024 and May 12, 2024, unauthorized individual(s) accessed and may have acquired your personal information, including your name and <<Variable Text 1>>.

LWC is committed to and takes very seriously, its responsibility to protect all data entrusted to it. As part of its ongoing commitment to the privacy of personal information in its care, LWC reviewed its existing policies and procedures and implemented additional safeguards to further secure its systems and the information contained therein. LWC is also notifying regulatory bodies and has notified and consulted with law enforcement.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements and credit reports for any anomalies. We also encourage you to review the enclosed *Steps You Can Take to Protect Your Personal Information* for additional guidance. You can also enroll to receive the **three (3) years of complimentary credit monitoring and identity restoration services** being offered to you.

To enroll:

- Call 1-866-980-5849 or visit https://app.idx.us/account-creation/protect and use the Enrollment Code provided above.

- IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note, the deadline to enroll is **January 17, 2025**.

Under U.S., law you are entitled to one free credit report annually from each of the three 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 major credit bureaus directly to request a free copy of your credit report.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

We understand that you may have questions or concerns that are not addressed in this letter. Please call the dedicated assistance line that we have established regarding this incident by dialing 1-866-980-5849 Monday through Friday from 9 am – 9 pm Eastern Time, excluding U.S. holidays.

LWC sincerely regrets any inconvenience or concern this incident may have caused you.

Sincerely,

Loring, Wolcott & Coolidge

Steps You Can Take to Help Protect Your Personal Information

Place a Fraud Alert

Consumers have the right to place an initial or extended "fraud alert" extended "fraud alert" on your 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	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-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Place a Security Freeze

As an alternative to a fraud alert, consumers have the right to place a "security 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 may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

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.);
7. Social Security Card, pay stub, or W2;
8. 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.

Should you wish to place a security freeze, please contact the three major credit reporting bureaus 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

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.