

# EXHIBIT 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, RGT Wealth Advisors, LLC (“RGT”) 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**

In November 2019, RGT became aware of unusual activity related to an employee’s email account. RGT immediately began an investigation, with the aid of third-party forensic specialists, to determine the nature and scope of the activity. Through the investigation, RGT determined that certain employee email accounts were subject to unauthorized access at various times between November 2, 2019 and November 15, 2019. Because the forensic investigation could not conclusively rule out access to data within the email accounts, in an abundance of caution, RGT undertook a lengthy and labor-intensive process to identify what information was present in the affected email accounts. Through this effort, the preliminary list of records was identified on August 25, 2020. After an extensive effort to reconcile the record and identify contact information, on or around November 23, 2020, RGT completed this review for certain individuals and began providing notice to impacted individuals as soon thereafter as possible.

The information that could have been subject to unauthorized access includes name and financial account information.

### **Notice to Maine Residents**

On or about December 21, 2020, RGT began providing written notice of this incident to affected individuals, which includes two (2) 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, RGT moved quickly to investigate and respond to the incident, assess the security of RGT systems, and notify potentially affected individuals. RGT is also working to implement additional safeguards and training to its employees. RGT is providing access to credit monitoring services for twelve (12) months through Kroll to Maine residents whose personal information was potentially affected by this incident, at no cost to these individuals. RGT will also be notifying other regulatory authorities, as required.

Additionally, RGT is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. RGT is 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 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.

# EXHIBIT A



RGT Wealth Advisors  
5950 Sherry Lane, Suite 600  
Dallas, Texas 75225  
www.rgtadvisors.com  
Phone: 214 360 7000  
Fax: 214 360 7010

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

**RE: Notice of <<b2b\_text\_1(SubjectLine)>>**

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

RGT Wealth Advisors, LLC (“RGT”) writes to inform you of an incident that may affect the privacy of some of your personal information. While we have no evidence of actual or attempted misuse of your information, we wanted to provide you with information about the incident, steps we are taking in response, and steps you may take to better protect your information, should you feel it is appropriate to do so. Please know we take this incident very seriously and have been working diligently to investigate and respond.

**What Happened?** In November 2019, RGT became aware of unusual activity related to an employee’s email account. We immediately began an investigation, with the aid of third-party forensic specialists, to determine the nature and scope of the activity. Through the investigation, RGT determined that certain employee email accounts were subject to unauthorized access at various times between November 2, 2019 and November 15, 2019. Because the forensic investigation could not conclusively rule out access to data within the email accounts, in an abundance of caution, RGT undertook a lengthy and labor-intensive process to identify what information was present in the affected email accounts. We then worked diligently to reconcile this information with our internal records in furtherance of identifying the individuals to whom the data relates and the appropriate contact information for those individuals. While this review is still ongoing, on or around November 23, 2020, we completed this review for certain individuals. RGT is notifying you because we understand, based on our investigation, that your information may have been present in the affected email accounts during the period of unauthorized access.

**What Information Was Involved?** Our investigation determined that this information may include your <<b2b\_text\_2(DataElements)>>. Again, we have no evidence of any actual or attempted misuse of your information; rather, we are letting you know in an abundance of caution and providing information and resources to assist you in protecting your personal information, should you feel it appropriate to do so.

**What We Are Doing.** We take this incident and the security of personal information in our care very seriously. We have security measures in place to protect the data on our systems and we continue to assess and update security measures and training to our employees to safeguard the privacy and security of information in our care. We are also notifying regulatory authorities, as required by law.

As an added precaution, we are also offering you access to 12 months of identity monitoring services through Kroll at no cost to you. Your identity monitoring services include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. If you wish to activate Kroll’s identity monitoring services, you may follow the instructions included in the “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 and to review your account statements and free credit reports for suspicious activity and to detect errors. We encourage you to activate the identity monitoring services through Kroll. Please also review the enclosed Steps You Can Take to Help Protect Your Information.

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 214-360-7000 and ask to speak to your RGT advisor if you have one.

Again, please know we take this incident very seriously and have been working diligently to investigate and respond. We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

RGT Wealth Advisors, LLC

## Steps You Can Take to Help Protect Your Information

### Activate Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. To activate:

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

### **ADDITIONAL DETAIL REGARDING YOUR 12 MONTH COMPLIMENTARY IDENTITY MONITORING SERVICES**

**Single Bureau Credit Monitoring** - You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

**\$1 Million Identity Fraud Loss Reimbursement** - Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

**Fraud Consultation** - You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Identity Theft Restoration** – If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

### Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and credit reports for suspicious activity and to detect errors over at least the next 12 to 24 months. 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](http://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.

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**

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://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 have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
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 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**

P.O. Box 9554  
 Allen, TX 75013  
 1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
 Chester, PA 19016  
 1-800-680-7289  
<https://www.transunion.com/fraud-alerts>

**Equifax**

P.O. Box 105069  
 Atlanta, GA 30348  
 1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://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](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); 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 Office of the District of Columbia Attorney General can be contacted at 400 6th Street, NW, Washington, DC 20001; Phone (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: [oag@dc.gov](mailto:oag@dc.gov); or you may visit the website of the Office of the District of Columbia Attorney General at <https://oag.dc.gov/>.

**For Maryland residents**, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or [www.oag.state.md.us](http://www.oag.state.md.us). RGT may also be contacted by mail at RGT Wealth Advisors, LLC 5950 Sherry Lane, Suite 600 Dallas, Texas 75225.

**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 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](http://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 Attorney General can 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 Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; or [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**For Rhode Island residents**, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; 1-401-274-4400; or [www.riag.ri.gov](http://www.riag.ri.gov). Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [There is/are approximately \[XX\] Rhode Island residents impacted by this incident.](#)