LIGHT TOWER FINANCIAL STRATEGIES LETTERHEAD

[January XX 2021]

[Client Name]

[Street Address]

[City, State, and Zip Code]

Dear [Client Name],

I’m writing to let you know that, on January 15, 2021, my computer was compromised. The data accessed may have included personal information, such as your full name, address, Social Security number, date of birth, email address, passport number, driver’s license number, and check-writing/debit card information.

Light Tower Financial Strategies values your business and respects the privacy of your personal information, and we deeply regret that this incident occurred. Upon detection, I immediately notified our broker/dealer, Commonwealth Financial Network®, who quarantined the device and escalated the issue for further forensic analysis. We have implemented additional security measures – including adding soft restrictions to your accounts – designed to prevent a recurrence of such an attack and to protect the privacy of Light Tower Financial Strategies’ valued customers.

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. The package includes the following benefits:

* Credit Monitoring
* Fraud Consultation
* Identity Theft Restoration

To take advantage of this offer, please contact me by email or phone. Please also review the enclosed instructions to learn more about how to protect your personal information.

If you have any questions or concerns, please contact me at 978.943.6393 between [TIME RANGE].

Sincerely,

Rebecca Linhart, AIF®, CeFT®

**Steps to Further Protect Your Information**

1. **Review your account statements and notify law enforcement of suspicious activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely and notifying your other financial institutions. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to *www.ftc.gov/idtheft* or call 877.438.4338. Complaints filed with the FTC will be added to the FTC’s Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

1. **Obtain a copy of your credit report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting *www.annualcreditreport.com*, calling toll-free 877.322.8228, or by completing an Annual Credit Report Request Form and mailing it to:

Annual Credit Report Request Service

PO Box 105281

Atlanta, GA 30348

You can print a copy of the request form at *https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf*. Or, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies:

Equifax Experian TransUnion

800.685.1111 888.397.3742 800.916.8800

*www.equifax.com www.experian.com www.transunion.com*

1. **Place a fraud alert on your credit report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at *www.annualcreditreport.com*.

1. **Put a security freeze on your credit file**

In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name and is designed to prevent fraudsters from accessing your credit report without your consent. However, this may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. And, you may be required to provide the consumer reporting agency with information that identifies you including your full name, social security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.

1. **Access additional free resources on identity theft**

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit *www.ftc.gov/idtheft* or call 877.438.4338. A copy of *Taking Charge: What to Do if Your Identity is Stolen*, the FTC’s guide to help you guard against and deal with identity theft, can be found on the FTC’s website at *www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm*.