16078

CAMBRIDGE TRUST

PRIVATE BANKING WEALTH MANAGEMENT

August 5, 2019

[redacted]

An Important Notice Regarding your Sensitive Customer Information

Dear [redacted],

Cambridge Trust Company is writing this letter to inform you of an information security incident involving the potential unauthorized access or potential use of your sensitive customer information.

Cambridge Trust has a comprehensive security program in place to guard against unauthorized access to our clients' sensitive information. However, the Bank was notified on August 2, 2019 about a processing error that occurred on that date at Cambridge Trust. This error may have resulted in certain information about your Cambridge Trust account being exposed to another party.

The information exposed would be your name and social security number. Cambridge Trust acted promptly and was able to contact the third party who received the information. The third party confirmed that your information has been deleted. However, there is a potential risk that fraud could be committed with the information that was revealed.

We recommend that you continue to carefully review your monthly statements and immediately alert us if you see anything suspicious. Using online banking will enable you to check your account activity even more frequently.

For more information, please visit an office that is convenient to you, or call our Customer Resource Center at 617-876-5500.

Sincerely,

James J. Zurn
Vice President
Digital Banking Manager

Guarding Against Identity Theft

Please be aware that even though we are notifying you of this situation, it does not necessarily result in you becoming a victim of identity theft. However, you do have an increased risk and we have outlined some steps below that you may take to protect yourself. While nothing can guarantee that you won't become a victim of identity theft, you can minimize your risk, and minimize the damage if a problem develops, by making it more difficult for identity thieves to access your personal information. The following list from the Federal Trade Commission ("FTC") describes ways in which incidents of identity theft can be mitigated:

- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- Never click on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spy ware, and anti-virus software to protect your home computer; keep them up-to-date. Visit http://www.OnGuardOnline.gov for more information.
- Don't use an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

You should remain vigilant in reviewing account activity over the next twelve to twenty-four months, and promptly report incidents of suspected identity theft to the Bank. Concurrently, the Bank's Fraud Unit will be monitoring all affected accounts. We recommend the following course of action:

a. Review account activity daily via the Bank's Online Banking service if possible and immediately report any suspicious activity to the Bank. If you are not an Online Banking user, be sure to review your account statements as soon as they arrive in the mail.

b. Consider placing a fraud alert with the credit reporting agencies to put your creditors on notice that you may be a victim of fraud. To place an alert on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your Social Security number, name, address and other personal information requested by the consumer reporting company. The credit reporting agencies may be reached at:

Equifax	1-800-525-6285	www.equifax.com	PO Box 740241 Atlanta, GA 30374
Experian	1-800-397-3742	www.experian.com	P.O. Box 9554

			Allen, TX 75013
TransUnion	1-800-680-7289	www.transunion.com	P.O. Box 6790 Fullerton, CA 92834

c. Periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted. You are entitled to receive one free credit report from each agency per year. For more information please visit the following website www.annualcreditreport.com. Information may also be obtained at 877-322-8228.

d. For more information on protecting yourself against identity theft, visit the FTC's website at www.consumer.gov/idtheft. Any incidents of identity theft should be reported to the FTC. Guidance from the FTC may also be obtained at 1-877-IDTHEFT.

e. You have the right to file a police report. File a police report and criminal complaint with your local police department and/or district attorney's office. Be sure to keep a copy of your filed complaint, as some creditors may request it for verification of your case.

Placing a Security Freeze on Your Credit Report

Any consumer in Massachusetts may place a security freeze on his or her credit report. A security freeze shall be requested by sending a request either by certified mail, overnight mail or regular stamped mail to a consumer reporting agency. The written request must:

- Provide your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number and date of birth.
- If you have moved in the past 5 years, supply the addresses where you have lived over the prior 5 years.
- Provide proof of current address such as a current utility bill or phone bill.
- Send a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.
- If you are not a victim, include payment by check, money order or credit card (Visa, Master Card, American Express, or Discover cards only).

Please see section "b" above for credit reporting agency addresses.

The credit reporting agency is not allowed to charge a fee to victims or their spouses for placing, removing for a specific period or party, or removing a security freeze on a credit report. To prove you are a victim, you must also send to the credit reporting agency a valid copy of a police report. All other consumers must pay a $5 fee for each placing, temporary lifting or removing of a security freeze.

A security freeze shall prohibit, with certain specific exceptions, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. The freeze goes into effect three business days from receipt of the consumer's letter by the credit reporting agency.

For more information regarding the security freeze please visit the following website http://www.consumerunion.org/pdf/security/securityMA.pdf .