BARNES & THORNBURG LLP

One North Wacker Drive
Suite 4400
Chicago, IL 60606-2809 U.S.A.
(312) 357-1313
Fax (312) 759-5646

www.btlaw.com

Michael Baumert
Attorney
(312) 214-4570
Michael.Baumert@btlaw.com

November 27, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Security Event Notice Provided for Indiana Trust and Investment Management Company

To whom it may concern:

Barnes & Thornburg LLP acts as attorneys for Indiana Trust and Investment Management Company ("Indiana Trust"), an entity incorporated in the State of Indiana and located at 4045 Edison Lakes Parkway, Mishawaka, Indiana, 46545, with respect to a data security event and the exposure of certain personal information as described in more detail below.

1. Nature of the Security Event

On August 12, 2019, Indiana Trust was the victim of a targeted phishing attack by malicious outside actors. The cybercriminals obtained unauthorized access to an email account of one of Indiana Trust's employees. Between August 12, 2019, and August 16, 2019, the attacker accessed the compromised email account.

Not a single transfer has been made from an Indiana Trust Account, and no other email account, system, network, or computer has been compromised.

2. Number of New Hampshire Residents Affected

One (1) of the affected individuals is a resident of New Hampshire and the information related to this individual may have included the names, Social Security numbers, birthdates, Passport Numbers, Driver's License information, email addresses, account numbers, and other financial information. Not all types of information were disclosed for all affected individuals.

3. Steps Taken or Planned to be Taken Related to the Security Event

Alerted by the suspicious email activity on August 16, 2019, Indiana Trust immediately took steps to neutralize the threat. Additionally, Indiana Trust immediately engaged outside counsel and forensic investigators to begin conducting an investigation to determine the scope of the incident. After a thorough review of the impacted email account and its contents, Indiana Trust identified any information that may have been accessed by the attacker within the compromised email account.

Indiana Trust has implemented additional security measures designed to remove the cybercriminals' access to its systems and to detect future threats. Indiana Trust has also implemented additional training and education for our staff in order to prevent the recurrence of such an attack.

Indiana Trust's investigation did not yield any evidence of additional existing threats. Indiana Trust will also continue to carefully monitor for signs of further activity or compromise. Indiana Trust is also providing resources, explained in the attached sample notification letter, to help protect against potential misuse of information.

As outlined in the attached breach notification letter, Indiana Trust has provided the affected individuals via U.S. Mail with the information related to their rights to place a security freeze on a credit report and to place a fraud alert. Indiana Trust will also provide affected residents of New Hampshire with Equifax ID Patrol credit monitoring service for the period of 12 months.

4. Contact Information

Please contact the undersigned with any questions regarding this incident.

Very truly yours,

BARNES & THORNBURG LLP

Michael Baumert

Michael Baumert

CC:
David R. Kibbe, Indiana Trust and Investment Management Company
Brian J. McGinnis, Barnes & Thornburg LLP

[ORGANIZATION LETTERHEAD]

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[DATE]

NOTICE OF DATA BREACH

Dear [INDIVIDUAL NAME]:

We are writing to inform you of a recent data security incident that has the potential to impact our current and previous clients. Although at this time we are not aware of any misuse of your information, we are providing this notice to ensure that you may take steps to protect your information should you feel it is appropriate to do so. We deeply regret that this incident occurred and take the security and privacy of our clients' information seriously.

WHAT HAPPENED?

On August 12, 2019, Indiana Trust and Investment Management Company ("Indiana Trust") was the victim of a targeted phishing attack by malicious outside actors. The cyber criminals obtained unauthorized access to an email account of one of Indiana Trust's employees. Between August 12, 2019, and August 16, 2019, the attacker accessed the compromised email account.

Not a single transfer has been made from an Indiana Trust Account, and no other email account, system, network, or computer has been compromised.

WHAT INFORMATION WAS INVOLVED?

Our investigation revealed the attackers may have accessed and/or duplicated the information within the compromised email account. This information included names, Social Security numbers, birthdates, Passport Numbers, Driver's License information, email addresses, account numbers, and other financial information. Not all types of information were disclosed for all affected individuals.

WHAT WE ARE DOING

Indiana Trust immediately took steps to neutralize the threat. Particularly, we immediately engaged outside counsel and forensic investigators to begin conducting an investigation to determine the scope of the incident. After a thorough review of the impacted email account and its contents, we identified any information that may have been accessed by the attacker within the compromised email account.

Indiana Trust has implemented additional security measures designed to remove the cyber criminals' access to our systems and to detect future threats. We have also implemented additional training and education for our staff in order to prevent the recurrence of such an attack. Our investigation did not yield any evidence of additional existing threats and we will continue to carefully monitor for signs of further activity or compromise. We are also providing resources, explained in this letter, to help protect against potential misuse of your information.

WHAT YOU CAN DO

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

Additionally, as a precaution we have arranged for you, at your option, to enroll in Equifax ID Patrol, a complimentary [*time*]-year credit monitoring service. This service provides: (i) daily credit monitoring of your Equifax, Experian and TransUnion credit files, (ii) unlimited access to your Equifax Credit Report, (iii) an annual 3-in-1 Credit Report which provides you with your credit history as reported by the three major credit reporting agencies, (iv) the ability to lock and unlock your Equifax credit file in real time, (v) the ability to set a fraud alert on your credit file at all 3 bureaus and automatically renew every 90 days, (vi) scans of the internet for your personal information and alerts if it is found on suspected underground trading sites, (vii) wallet replacement assistance in the event of a lost/stolen wallet, and (viii) identity theft insurance up to $1,000,000 to cover certain out of pocket expenses arising from an occurrence of identity theft, subject to certain limitations and exclusions. You have until [*date*] to activate the free, optional service by using the following activation code: [*code*]. This code is unique for your use and should not be shared. Please go to [*enrollment info*] or call [*call-in number*] to enroll.

FOR MORE INFORMATION

We sincerely regret the inconvenience and concern this incident may cause you. If you have questions not addressed by this letter, please do not hesitate to contact the call center we have established at [*telephone number*]/[*toll-free number*]] between [8:00] a.m.- [5:00] p.m. EST from Monday through Friday.

Sincerely,

David R. Kibbe
President & CEO

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

1) Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

You should always remain vigilant for incidents of fraud and identity theft. Over the next twelve to twenty four months, we recommend that you remain especially vigilant by reviewing your account statements and credit reports closely. 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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (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.

2) Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://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, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at:
https://www.annualcreditreport.com/requestReport/requestForm.action.

Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies, for the purpose of requesting a copy of your credit report or for general inquiries, is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

3) Consider Placing 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 one year. 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 http://www.annualcreditreport.com.

4) Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information.

Additional information is available at:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

A copy of *Identity Theft – A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

5) Security Freeze

In all US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, 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. There is no charge to request a security freeze or to remove a security freeze.

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services/

6) MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with, and shredding receipts, statements, and other sensitive information.

7) USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.