What Happened:

On July 15, 2021, the Buddhist Tzu Chi Foundation and its affiliated organizations Buddhist Tzu Chi Education Foundation and Buddhist Tzu Chi Medical Foundation (collectively referred to as "Tzu Chi" or as first person) discovered certain of our computer systems were behaving abnormally. Upon discovery, we immediately contacted local and Federal law enforcement and began working with third-party specialists to determine the source of the incident and extent of systems affected. To the best of our knowledge the Donation Information System was not compromised.

Preliminary investigation determined that Tzu Chi was a victim of a ransomware attack. As the result certain systems containing private and confidential information have been compromised.

What Information Was Involved:

Since July 15, 2021, ongoing investigations with our incidence response partners have determined that compromised data may include: Social Security Numbers; Driver's License Numbers; California identification card numbers; passport numbers; military identification numbers; financial information; medical information; health insurance information; and/or information or data collected through under various programs offered by us in the past. Although we have no evidence of actual or attempted misuse of information at this time, we are taking steps to notify our staff, volunteers, vendors, clients and other parties that may be impacted out of an abundance of caution.

What is the Tzu Chi Doing to Address the Issue?

We are reviewing our network security polices and are taking immediate steps to further enhance its security. We take privacy and security of all information very seriously. The Foundation is also establishing a dedicated assistance line to answer your questions and to provide credit monitoring services to potentially impacted individuals.

What Can Potentially Impacted Individuals Do?

We encourage individuals to remain vigilant and regularly review and monitor their credit reports/account statements for suspicious activity and to detect errors. Additionally, individuals

can review the below steps to protect their information and contact the dedicated assistance line to obtain enrollment information for the credit monitoring services being offered.

For More Information:

Tzu Chi has established a dedicated assistance line to address any questions individuals may have and to provide credit monitoring services to potentially impacted individuals. The assistance line can be reached at 888-xxx-9999 Tuesday through Saturday 9 a.m. to 5 p.m. Pacific Time.

The following information is provided to help individuals wanting more information about steps that they can take to protect their information:

What steps can I take to protect my private information?

- If you detect suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.

- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll free at 1-877-xxx-8228.

Contact information for the three agencies appears at the bottom of this page.

- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

How do I obtain a copy of my credit report?

Visit www.annualcreditreport.com or call 1-877-xxx-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

How do I place a Fraud Alert on my account?

You may need to contact one of the major credit reporting companies for assistance. An initial one-year security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender may be required to take steps to verify that you have authorized the request. Please contact the agencies for additional information and details.

TransUnion Fraud Alert, 1-800-680-7289, www.transunion.com
P.O. Box 2000, Chester, PA 19016-2000
Experian Fraud Alert, 1-888-397-3742, www.experian.com
P.O. Box 9554, Allen, TX 75013
Equifax Fraud Alert,1-888-298-0045, www.equifax.com
P.O. Box 105069, Atlanta, GA 30348-5069

How do I place a Security Freeze on my account?

Please contact one of the major credit reporting companies for assistance. security freeze prevents your credit report from being accessed with some exceptions. A security freeze needs to be lifted each time you apply for credit.

To request a credit freeze, you may need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.).
2. Social Security number.
3. Date of birth.
4. Address for the prior two to five years.
5. Proof of current address, such as a current utility or telephone bill.
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement

agency concerning identity theft, if you are a victim of identity theft.

*Actual information needed may vary between the credit agencies and the above list is for reference only.

TransUnion Credit Freeze, 1-800-680-7289, www.transunion.com
P.O. Box 160, Woodlyn, PA 19094
Experian Credit Freeze, 1-888-397-3742, www.experian.com
P.O. Box 9554, Allen, TX 75013
Equifax Credit Freeze, 1-888-298-0045, www.equifax.com
P.O. Box 105788, Atlanta, GA 30348-5788

What is the difference between a 'Fraud Alert' and a 'Security Freeze'?

A fraud alert notifies anyone requesting your credit file that you suspect you are a victim of fraud. As such, the lender should take steps to verify that you have authorized the request and deny any request that cannot be verified.

A security freeze will prevent lenders and others from accessing your credit report completely.