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

NOTICE OF SECURITY INCIDENT

Dear XX,

We are writing to let you know about a data security incident that may involve your personal information. We found no evidence of any fraudulent access or misuse of your personal information, but we wanted to inform you of this situation out of an abundance of caution.

WHAT HAPPENED?

In early July 2023, an unauthorized external party posted the presumed direct internet links to a limited portion of The Columbus Foundation's ("TCF") internal data related to our Gifts of Kindness and external Emergency Assistance programs.

Although TCF does not require any personally identifiable information ("PII") in connection with its Emergency Assistance Program or Gifts of Kindness applications, and goes to great lengths to minimize the amount of PII received by deploying various tools to identify and remove such information, documents containing PII are sometimes submitted by applicants or partner organizations and stored alongside other application materials. Based on a document and data review, the linked data included some of your PII provided by you or a nonprofit partner in conjunction with applications to either the Gifts of Kindness or Emergency Assistance programs.

WHAT INFORMATION WAS INVOLVED?

The potentially compromised data identified by investigators included applicants' name, address, driver's license number, and Social Security number. While this information may have been accessible online, at this time there is no evidence of any fraudulent access or misuse of the affected information.

WHAT WE ARE DOING

Immediately upon learning of the potential PII data exposure, TCF removed all access to the relevant information. Data that may have been accessible through the posted links was removed and verified to no longer be accessible. Again, TCF has not found any evidence that any of your data was fraudulently accessed or misused. TCF has worked closely with outside legal counsel and technical resources to examine the source, accessibility, nature, and scope of the potential data exposure to ensure all appropriate steps were taken.

TCF regularly evaluates its security measures and engages expert service providers to ensure our systems maintain a high level of security. To this end, going forward, TCF is also taking additional steps to further ensure that PII is not inadvertently shared by applicants during the Gifts of Kindness and Emergency Assistance application intake processes and related procedures. TCF's review of the potentially affected records and related internal processes will continue and you will be notified of any new information about this matter that is material to your interests. In the meantime, although based upon on our investigation and the guidance of our outside experts we believe that it is unlikely that your PII was compromised, we encourage you to review and take advantage of the enclosed resources.

Furthermore, while we do not believe that misuse of your information has occurred, as an added precaution we are offering twelve (12) months of identity and credit monitoring at no cost to you through Experian. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by December 31, 2023 (your code will not work after this date).
- Visit the Experian IdentityWorks website at https://www.experianidworks.com/3bcredit
- Provide your activation code: [CREDIT MONITORING PROMOTION CODE]

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, believe there was fraudulent use of your information as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by December 31, 2023. Experian agents can assist you in resolving each incident of fraud from the date of the incident including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition. Be prepared to provide engagement number B103810 as proof of eligibility for the Identity Restoration services by Experian.

WHAT YOU CAN DO

It is recommended that you monitor your account statements and credit reports closely, and place a credit freeze as detailed below. You may take advantage of free credit monitoring and identity theft protection services as outlined above. Please also 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.

FOR MORE INFORMATION

For further information and assistance, please contact The Columbus Foundation's Data Desk at (614) 251-4013.

Sincerely,

The Columbus Foundation

Steps You Can Take to Further Protect Your Information

- **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. 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.

- **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 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 Atlanta, GA 30374	P.O. Box 2002 Allen, TX 75013	2 Baldwin Place P.O. Box 1000 Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

We recommend 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.

- **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://consumer.ftc.gov/identity-theft-and-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.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222

OTHER IMPORTANT INFORMATION

- **Security Freeze**

In some 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.

- **Exercise Your Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) Rights**

In the event a business provides credit, goods, or services to someone fraudulently using your information, you may request that business provide the records relating to that transaction to you and/or law enforcement.

For more information, visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.