



Richard Goldberg, Partner & Vice-Chair
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
rgoldberg@constangy.com
Mobile: 917.744.1760

February 20, 2024

VIA Portal:

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith and Prophete LLP ("Constangy") represents T.Y. Lin International Group ("T.Y. Lin") with corporate headquarters located in San Francisco, CA in connection with an incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with your data privacy laws.

1. Nature of the Security Incident

On August 1, 2024, T.Y. Lin experienced a network disruption due to a ransomware attack and immediately initiated an investigation of the matter. T.Y. Lin engaged cybersecurity experts to assist with the process. The investigation revealed that an unauthorized actor had access to certain files from the T.Y. Lin network on or about July 27, 2023. After receiving the preliminary forensic findings, T.Y. Lin immediately communicated details of the incident to any potentially impacted staff and provided them with credit monitoring services on August 9, 2023.

After a diligent search, which included data mining efforts, T.Y. Lin confirmed the full identities and addresses of potentially impacted individuals and their personal information data types on February 12, 2024. This personal data was stored in the network environment and may have been accessible to the unauthorized actor while they were in the network environment. T.Y. Lin has no information indicating the information involved has been or will be published, shared, or otherwise misused.

2. Number of Affected MD Residents & Information Involved

February 20, 2024
Page 2

After researching additional address information, T.Y. Lin notified 15 residents on February 20, 2024. A sample copy of the notification letter is included with this correspondence. The potentially affected information varied by individual but included the following: Social Security numbers. T.Y. Lin has no reason to believe that the information involved has been or will be published, shared, or otherwise misused.

3. Notification to Affected Individuals

On February 20, 2024, a notification letter was sent to the affected residents by USPS First Class Mail. The notification letter provides resources and steps the individual can take to help protect their information. The notification letter also offers 12 months of complimentary identity protection services including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

Upon discovering the issue, T.Y. Lin notified potentially impacted staff and provided them with credit monitoring service. T.Y. Lin's management also communicated the details of the incident and provide points of contact for questions as well. Finally, T.Y. Lin engaged in a diligent search of its international networked environment and enlisted the assistance of several management teams at its many office locations.

In addition, T.Y. Lin is providing a second complimentary credit monitoring and identity protection services through Experian, the data breach and recovery services expert to affected individuals, whose social security numbers were impacted. These services include 12 months of credit monitoring, identity protection, and fully managed identity theft recovery services. With this protection, Experian will help them resolve issues if their identity is affected.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at RGoldberg@constangy.com or 917.744.1760.

Sincerely,



Richard Goldberg
Constangy, Brooks, Smith & Prophete LLP

RG:jsc

Encl.: Sample Notification Letter

cc: Jason S. Cherry, Constangy (jcherry@constangy.com)



Return Mail Processing
PO Box 999
Suwanee, GA 30024

8 1 2388 *****SINGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



February 20, 2024

RE: Data Security Incident

Dear Sample A. Sample:

We are writing to notify you about a cybersecurity incident experienced by TYLin International Group, Ltd. (“TYLin”), which may have affected your personal information. TYLin takes this matter extremely seriously. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened: On February 12, 2024, we determined that your information may have been involved in a data security incident. On August 1, 2023, the company experienced a network disruption and immediately initiated an investigation of the matter. The company engaged independent cybersecurity experts to assist with the process. The investigation revealed that an unauthorized actor may have accessed certain files from the company network. On August 9, 2023, although we did not know if any personal information was involved in the incident, out of an abundance of caution the company immediately provided our employees with free identity protection services. We then continued the investigation to determine whose data may have been involved in the incident and worked to provide notification to the correct people.

What Information Was Involved: The information involved may have included your name and [Extra1]. Please note that we have no evidence of any actual or suspected misuse of this information.

What We Are Doing: As soon as TYLin discovered the incident we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable. We are also offering you complimentary credit monitoring and identity protection services through Experian, a leader in consumer identity protection for [Extra2] months. These services include credit monitoring, identity protection through IdentityWorksSM, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Note: if you previously signed up for credit monitoring in August of 2023, you may open another credit monitoring account under a different email address for an additional [Extra2] months of coverage.

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by May 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose 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 833-918-1096 by May 31, 2024. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do: We encourage you to enroll in the complimentary credit protection services we are offering. With this protection, Experian can help you resolve issues if your identity is compromised. Please also review the guidance included with this letter which contains additional resources you may utilize to help protect your information.

TYLin is taking this matter extremely seriously and deeply regrets any worry or inconvenience that this may cause. If you have any questions, please contact 1-833-918-1096 by May 31, 2024. Be prepared to provide engagement number [Engagement Number].

Very truly yours,

A handwritten signature in dark ink, reading "Ian R MacLeod". The signature is written in a cursive, flowing style.

Chief Human Resources Officer
TYLin International Group, Ltd.

ADDITIONAL DETAILS REGARDING YOUR [Extra2]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

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 in Experian IdentityWorks:

- **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 file 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 high-level of 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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE TO HELP 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of 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 <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 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>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave,
NW Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General 150

South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.