Lowenstein Sandler

Erich J. Kaletka
Associate

One Lowenstein Drive
Roseland, New Jersey 07068

April 5, 2024

BY EMAIL

Attorney General John Formella
Consumer Protection Bureau
Office of the Attorney General
1 Granite Place
South Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Data Incident

To Whom It May Concern:

We write on behalf of our client, TOCCI Building Corporation, to inform you of a recent security incident that may have affected the personal information of one New Hampshire resident.

On February 29, 2024, TOCCI discovered that it was the target of a ransomware incident in which an unauthorized person gained access to certain of its systems, encrypting numerous servers and leaving behind ransom letters demanding payment in exchange for the restoration of functionality and data.

The personal data on the impacted systems included

TOCCI's team worked diligently to minimize the impact on their servers and operations, and to restore functionality. They notified law enforcement and have engaged an outside firm and forensics experts to investigate the scope and impact of the incident, including investigating what types of data were compromised.

We have attached sample notification made to the affected parties. This notice advised on credit monitoring, credit freezes, and identity theft prevention services. If you have any questions, please reach out to us.

Sincerely,

Erich J. Kaletka
Attachment

Re: Notice of Data Breach

TOCCI BUILDING CORPORATION is letting you know about a recent data breach. We are notifying you of this incident and providing you with tools and guidance to help you protect yourself against potential risk of identity theft and fraud. We are currently aware of data loss relating to the time period 2010-2015, but we are continuing to investigate. Potentially you worked on a project in New Jersey for the construction of the Peter W. Rodino Building located in Newark, NJ. You are being notified because we have reason to believe that some of your personally identifiable information may have been compromised because of these incidents.

What Happened

On February 29, 2024, we discovered that TOCCI BUILDING CORPORATION was affected by a data breach. The breach affects the personally identifiable information of approximately 500 individuals across approximately 14 US states. This breach resulted from a ransomware attack on our systems. Our team worked diligently to minimize the impact on our servers and operations, and to restore functionality. We have engaged an outside firm and forensics experts to investigate the scope and impact of the incident, including investigating what types of data were compromised. We are notifying you of this incident and providing you with guidance to help you protect yourself. We describe the available services below.

What Information Was Involved

We have thoroughly analyzed the compromised data and this event may have exposed some or all of the following:

What We Are Doing

Immediately upon learning of the problem, we began reviewing all aspects of the incident, and taking steps to protect our systems and everyone involved. We reported the incident to law enforcement and are working closely with outside experts to restore any damage sustained. We are taking this opportunity to review and, if necessary, to enhance system security and governance practices to help prevent a recurrence of future incidents.

TOCCI

We recommend you subscribe to a credit monitoring service. These plans typically have the following minimum coverages: 24/7 live support, daily credit monitoring, dark web monitoring, insurance reimbursement, and id theft recovery services. In the event you experience or suspect loss, this protection will help you monitor and resolve issues if your identity is compromised.

What You Can Do

As always, we recommend that you remain vigilant and review your account statements and credit reports regularly and report any concerning transactions to your financial services provider.

- Consider changing passwords to all your financial institutions and credit cards as a precaution.
- Review your credit reports.

To obtain a free annual credit report, go to www.annualcreditreport.com, or, the reporting agencies listed below are also free to register where you can get free updated credit reports.

- If you discover any suspicious items and have enrolled in a credit monitoring service, notify them immediately by calling or by logging into the website and filing a request for help.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your State's Attorney General, or the Federal Trade Commission ("FTC"). The FTC also provides a number of free resources for individuals affected by or concerned about identity theft. The FTC's toll-free telephone number and website are below:

Toll-Free Telephone Number:	+1 (877) 438-4338
Web address:	https://www.identitytheft.gov/#/

We also advise you to place fraud alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at any one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Equifax Fraud Reporting 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013

www.experian.com

TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well, then you will receive confirmation letters in the mail. An initial fraud alert will last for one year. Please Note: No one is allowed to place a fraud alert on your credit report except you.

Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

Please reach out if you have any questions about the above information.

Sincerely,

Paul Neenan, CFO

TOCCI BUILDING CORPORATION