



Shopping Cart Elite

Dear [REDACTED]:

Setuno, Inc. d/b/a Shopping Cart Elite (“Setuno”) provides website shopping cart hosting services to retailers, including Concrete Countertop Solutions. We are writing to make you aware of a recent data security incident involving potential unauthorized access to some payment card data. The privacy and security of your personal information is of utmost importance to Setuno, and we are routinely evaluating and improving our security and payment systems to ensure your information is secure.

What Happened?

We recently discovered that our e-commerce platform was modified with malicious code that acted to capture payment card data as it was entered in connection with a purchase. We immediately engaged external forensic investigators and data privacy professionals and commenced a prompt and thorough investigation into the incident. As a result of this review, we determined that payment card information was potentially accessed related to transactions made between May 4, 2020 and May 11, 2020 at the above-listed retailer’s website.

What Information Was Involved?

The information that may have been impacted in this incident included customer name, credit or debit card numbers, card expiration dates and CVVs (3 or 4 digit code on the front or back of the card). Our investigation concluded on January 29, 2021 that you completed a transaction at the above-listed retailer’s website during the window of compromise and your card information may be at risk. No other personal information of yours is at risk as a result of this incident.

What We Are Doing

We wanted to make you aware of the incident, to let you know what we are doing to further secure your information, and to suggest steps you can take. Since learning of the incident, we have implemented enhanced security safeguards to help protect against similar intrusions. We are also conducting ongoing monitoring of our e-commerce platform to ensure that it is secure and cleared of any malicious activity.

What You Can Do

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

As a best practice, you should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you.

For More Information

Your trust is a top priority for Setuno, and we deeply regret the inconvenience this may have caused. The privacy and protection of information is a matter we take seriously.

**If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line to respond to questions at [REDACTED].** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8 a.m. to 5 p.m. Eastern Time.

Thank you,

[REDACTED]

**- OTHER IMPORTANT INFORMATION -**

**1. Placing a Fraud Alert.**

You may place an initial one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

**Experian**

P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

**TransUnion LLC**

P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
1-800-680-7289

**2. Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

**Equifax Security Freeze**

PO Box 105788  
Atlanta, GA 30348  
<https://www.freeze.equifax.com>  
1-800-349-9960

**Experian Security Freeze**

PO Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
1-888-397-3742

**TransUnion Security Freeze**

P.O. Box 2000  
Chester, PA 19016  
<http://www.transunion.com/securityfreeze>  
1-888-909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

**3. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. 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.

**4. Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.