



May 29, 2019

Dear Customer,

We are writing to you because of a potential threat to customer personal information. We have been notified by federal and state agencies that there may have been a breach of our customer information system, specifically concerning our automatic payments, potentially exposing customer personal information, such as customer names, e-mails, credit card, debit card, or other financial account information. Although we are not aware of any actual misuse of your information, we are providing notice to you and other potentially affected customers about steps you can take to protect yourself against possible identity theft or fraud.

What happened?

On May 28, 2019, we were informed of a possible data breach from the Department of Homeland Security. Homeland Security conveyed information suggesting that a hacker may have copied customer information through a software vulnerability in our customer information system provider.

What personal information was involved?

As noted above, we believe that the actors potentially had access to the following information: your first and last name, your credit card, debit card, or financial information, with associated access credentials and expiration dates, that was provided to the Lewes BPW for automatic payments, and your e-mail address.

What are we doing about it?

Upon receiving notice of this apparent breach, we immediately isolated the computer system in question and began compiling information to notify all affected customers. All affected customers are receiving an e-mail, phone call, and letter informing them of this breach. We have also notified our software vendor and are actively working with said vendor to identify and secure the suspected breach. Once we have identified and corrected the vulnerabilities we will then test and bring the system online. In addition, we have been in contact with state and federal agencies regarding the incident.



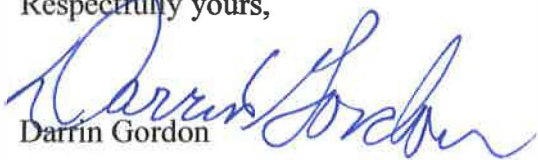
What can you do to protect yourself?

To protect yourself from the possibility of identity theft or fraud, we recommend that you immediately contact your credit or debit card company, or bank as the case may be, and inform them that your information may have been compromised, and to follow any steps they may recommend. We also recommend that you review your credit card and banking statements and report any suspicious activity to your financial institution. And please consider changing password and security questions on affected accounts.

These are precautionary measures that we have taken to ensure the security and safety of your information. We are not trying to cause undue concern, yet out of an abundance of caution we are being as open and forthcoming as possible. This will not have any effect on our ability to continue to provide first class electric, water, sewer and stormwater services.

Please do not hesitate to contact us at (302) 645-6228 for more information or if you have any questions.

Respectfully yours,


Darrin Gordon
General Manager