SAMPLE DATA BREACH NOTIFICATION

[Customer First Name] [Customer Last Name]

[Address 1]

[Address 2]

[City, State, Zip]

NOTICE OF DATA BREACH

Dear Customer,

We are writing to you because of an incident involving access to information associated with online purchases made on our website www.glasswasherparts.com. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected customers about the incident, and about tools you can use to protect yourself against possible identity theft or fraud.

What Happened?

We were informed on February 6, 2017 that our website www.glasswasherparts.com experienced an intrusion last year. Our site is operated for us by a third-party company (our "platform provider"), and it was the platform provider's systems that experienced the intrusion. The intruder or intruders placed malware on the platform provider's servers, and by doing so gained access to our customers' payment card data. To date, the investigation indicates that the intrusion began in approximately February 2016 and ended in December 2016. The attackers gained access to customer information including payment card numbers as customer made transactions on the platform provider's systems, and had access to historical payment card data. Because you have provided your payment card information to us in the past, we are notifying you about this data breach.

You may wonder why you are hearing about the breach now. The platform provider for www.glasswasherparts.com did not discover the breach until November. In addition, law enforcement is investigating, and asked that notification to customers be delayed to allow the investigation to move forward.

What Information Was Involved?

The information that the attacker had access to includes your first and last name, your address, your phone number and any debit or credit card numbers with expiration dates you may have used on our website.

What Are We Doing?

Our platform provider has worked with a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard personal information. Our platform provider has also contacted and offered its cooperation to federal law enforcement.

What You Can Do?

To protect yourself from the possibility of identify theft, we recommend you immediately contact your credit or debit card company and inform them that your card information may have been compromised, so that they can issue you a replacement card. Review your banking and card statements and report any suspicious activity to the relevant financial institutions.

For more information on identify theft, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov.

For More Information

If there is anything else that we can do to assist you, please call 954-960-1468 weekdays between the hours of 10am and 5pm.