TONKON TORP

Eric Beach
Of Counsel
503.802.2182 direct
503.221.1440 main

November 27, 2018

TO: State of Washington Office of the Attorney General
Consumer Protection Division

Re: Burgerville LLC – Data Breach Notification

This letter is to notify you of a breach of the Burgerville LLC company systems that resulted in the compromise of consumer payment card information.

On August 22, 2018, Burgerville was contacted by the FBI regarding a breach of payment card information by the international hacking organization Fin7. In cooperation with the FBI, Burgerville immediately launched a full forensic investigation with the assistance of a team of third-party cybersecurity professionals. Burgerville agreed to maintain the confidentiality of the breach as part of an active law enforcement investigation and to ensure that all pathways that the hackers were using could be identified and removed.

On September 19, 2018, Burgerville's investigation revealed that the breach was still active and that the initial intrusion into the system occurred in August 2017. The company immediately began steps to remediate the breach, neutralize the malware on its systems, and ensure that all access points to the hackers were effectively removed.

On September 30, 2018, Burgerville completed its remediation plan. The operation had to be kept confidential until it was completed in order to prevent the hackers from creating additional covert pathways into the company's network.

This intrusion was focused on credit and debit card information. Data compromised included names, card numbers, expiration dates, and the CVV numbers found on the back of most cards. There is no evidence of any other personal information being compromised.

On October 3, 2018, because Burgerville does not have contact information for the payment card holders affected by the breach, notice was provided to consumers via Burgerville's website and notice to media was made.

Because of the tactics of this particular group of hackers, it is impossible to say how many consumers in general and Washington residents in particular are impacted by this breach. Consumers have been notified that if they visited a Burgerville restaurant between August 2017 and September 30, 2018, they should closely monitor their debit and credit card activity.

Attached is the notification that was and still is being provided to consumers on Burgerville's website.

TONKON TORP LLP

By Eric C. Beach
Eric Beach

039752/00016/9494742v1

Important Security Information

Thank you for reaching out to learn more about the security breach at Burgerville.

We realize that this intrusion was not only on Burgerville's system, but also on your life. This isn't what you expected to happen when you came to visit one of our locations.

Beyond a breach of information, this type of intrusion impacts our way of life together. Feeling safe and having trust, these are core tenets of building a resilient community. From our mission: Serve With Love, we stand committed to being a good partner and helping to build confidence with the community that has given us so much.

Please take a moment to read through the Frequently Asked Questions below. After reading this information, if you still have additional questions, do not hesitate to call ***1-855-336-6688*** *(tel:1-855-336-6688) (toll-free, US only), Monday through Saturday, 6:00am-6:00pm (PST).*

Yours with love,
Jill Taylor, Interim CEO, Burgerville

Frequently Asked Questions

What happened?

On August 22, 2018, the Federal Bureau of Investigation (FBI) notified Burgerville of a cybersecurity breach impacting a number of the company's systems. The breach was perpetrated by Fin7 and was a sophisticated attack targeting companies with locations in the Pacific Northwest. Burgerville agreed to cooperate fully with the FBI investigation, and immediately began a forensic investigation of its own to determine the full extent of the breach.

On September 19, 2018, as part of its forensics investigation, Burgerville discovered that the breach, which was initially thought to be a brief intrusion, was still active. The group of hackers had placed malware on Burgerville's network and were continuing to collect payment data. Burgerville immediately began taking steps to contain the breach and disable the malware with the help of a third-party team of cybersecurity experts and in cooperation with the FBI.

What data was involved?

Over the course of the investigation, it was determined that some of Burgerville's customers' credit and debit card information, including names, card numbers, expiration dates, and the CVV numbers found on the back of most cards may have been compromised.

What has Burgerville done to stop this?

From the moment Burgerville was contacted by the FBI, the company has been fully engaged in a forensic investigation. As soon as Burgerville learned the malware was still in effect, a multi-phase remediation plan was activated. This has included cutting off the various pathways the intrusion affected and upgrading systems to eradicate this breach.

Who does this impact?

This intrusion was focused on credit and debit card information. There is no evidence of any other personal information being compromised. Burgerville is working with its customers and employees to address the effects of this incident.

Who did this?

The organization responsible for this breach is believed to be Fin7, a sophisticated international cybercrime group. On August 1, 2018, the U.S. Department of Justice issued a press release (https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100) announcing the apprehension of three members of this group who have been connected with launching cyberattacks on more than 100 companies across 47 states. The press release mentions that there was a wave of attacks on local businesses specifically in Western Washington, which includes Burgerville.

How many customers are affected?

The tactics of this particular group of hackers make it very difficult to know exactly how many people were directly affected and exactly which card numbers were stolen. They are adept at concealing their digital footprints. Since we can't say specifically which card numbers were taken, we encourage everyone who used a card at a Burgerville location between September 2017 and September 30, 2018, to closely monitor their debit or credit card activity.

Will Someone Be Contacting Me Directly Regarding The Breach?

No one should be contacting you unless you first initiated contact.

* Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact and are sure you know who you're dealing with.

* If you receive an email with a link or enter a transaction online, confirm that you are dealing with a legitimate organization before sharing any personal information. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or, call their customer service using the number listed on your account statement or in the telephone book.

* Beware of links in emails. If you see a link in a suspicious email link, don't click on it. Hover your mouse on the link without clicking it to see if the hyperlinked address matches the link that was typed in the message.

What do I need to do to make sure my information is secure?

If you have used a credit or debit card at Burgerville between September 2017 and September 30, 2018, you should:

* Review your card statements for any unauthorized charges. If you see something suspicious, contact your credit or debit card company immediately to report the activity.

* Set up credit/debit card account alerts. They are often the fastest and most effective way for you to know if there are fraudulent charges being made on your existing credit/debit card account, as these types of alerts provide real-time information to you about transfers, payments, and other transactions being made. Almost every bank and credit/debit card issuer provides account alerts for free as a service to consumers, and you can usually set them up by logging in to your online credit/debit card account or calling the telephone number on your card or statement.

* Obtain a copy of your credit report and look for unauthorized activity there, too. You can get a free copy of your credit report once every 12 months from each of the three top credit reporting agencies. To obtain your annual free credit report, please visit www.annualcreditreport.com (https://www.annualcreditreport.com/) or call **1-877-322-8228** (tel:1-877-322-8228).

* You may also want to consider freezing your credit. As of September 21, 2018, freezing your credit is a free service provided by the three major credit bureaus. Go to each of the credit bureau websites linked below and locate the security freeze information.

- For Equifax: www.equifax.com/personal/credit-report-services/ (https://www.equifax.com/personal/credit-report-services/)
- For Experian: www.experian.com/freeze (https://www.experian.com/freeze/)
- For TransUnion: www.transunion.com/credit-freeze (https://www.transunion.com/credit-freeze)

*** Burgerville has set up additional support online at burgerville.allclearid.com (https://burgerville.allclearid.com/) and though a service center which can be reached by calling 1-855-336-6688 (tel:1-855-336-6688) (toll-free, US only), anytime between the hours of 6:00am-6:00pm (PST) Monday through Saturday.**

What has Burgerville done to remediate this security breach?

Burgerville has neutralized the malware placed on its network during the breach. The company will continue to work with its cybersecurity firm to evaluate and upgrade its security systems.

Why Was Burgerville Storing Credit Card Numbers?

Burgerville doesn't store customers' credit card numbers. The malicious software that was installed on its system by the hackers does. This malicious software has been fully contained.

What other companies are affected?

Other than those who have publicly disclosed data breaches, as named in the Justice Department's press release, Burgerville has not been provided the names of any other impacted companies.

Why are you just informing us now?

The timeline of events is as follows:

August 22, 2018: Burgerville was contacted by the FBI regarding a data breach that had occurred in September 2017, a year ago. It was believed to have been a brief intrusion that no longer existed. In cooperation with the FBI, Burgerville immediately launched a full forensic investigation with the assistance of a team of cybersecurity professionals. Burgerville agreed to maintain the confidentiality of the breach as part of an active law enforcement investigation and to ensure that all pathways that the hackers were using could be identified and removed. Though this investigation, Burgerville was able to provide valuable evidence to the FBI.

September 19, 2018: Burgerville's investigation revealed that the breach was still active. The company immediately began steps to remediate the breach, neutralizing the malware on its systems and ensuring that all access points to the hackers were effectively removed.

September 30, 2018: Burgerville completed its remediation plan. The operation had to be kept confidential until it

was completed in order to prevent the hackers from creating additional covert pathways into the company's network.

This was a sophisticated attack in which the hackers effectively concealed all digital traces of where they have been. However, in an abundance of caution, Burgerville recommends that anyone who visited their restaurants between September 2017 and September 2018 should consider that their data may have been compromised.

Updated at 4:24 am, Oct. 12, 2018