PRESS RELEASE

FOR IMMEDIATE RELEASE

Islands Restaurants Announces Payment Card Incident

CARLSBAD, CA – December 19, 2019 – Islands Restaurants was alerted to a potential payment card issue, immediately started an investigation, and took steps to end unauthorized access to our payment card network. A leading computer forensic firm was engaged, and a thorough investigation was conducted to determine what occurred and what restaurant locations and time frames were involved. Islands notified the card networks and provided information to support an investigation by law enforcement.

Over the general time frame of February 18, 2019 to September 27, 2019, malware was installed on certain point-of-sale devices in our restaurants that were used for payment card transactions. The time frames involved vary by restaurant. Not all Islands restaurants were involved, and for some restaurants some but not all devices were involved. And at many of the restaurants involved, cards were not successfully obtained during certain weeks in March 2019. So, it is possible that not every card used at a restaurant during the time frame involved was found by the malware.

The malware was designed to look for data read from the magnetic stripe of a payment card as it was being routed through the system. Data in the magnetic stripe includes the cardholder name, card number, expiration date, and internal verification code. In some instances, the malware only identified the portion of the magnetic stripe that contained payment card information without the cardholder name.

Lists of the restaurants involved and their respective time frames are available at:

www.islandsrestaurants.com/paymentcardnotification

This site also provides information about the incident and additional steps customers may take.

Islands quickly took measures to contain the incident, remove the malware, and has been working to implement measures to further enhance payment card security. It is always advisable to remain vigilant to the possibility of fraud by reviewing payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued your card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card.

For more information regarding this incident, customers may visit the sites listed above or call 833-935-1380 Monday through Friday between the hours of 6:00 a.m. to 6:00 p.m. Pacific Time.

ISLANDS RESTUARANTS SUBSTITUE NOTICE

Notice of Data Breach

What Happened?

Islands Restaurants was alerted to a potential payment card issue, immediately started an investigation, and took steps to end unauthorized access to our payment card network. A leading computer forensic firm was engaged, and a thorough investigation was conducted to determine what occurred and what restaurant locations and time frames were involved. Islands notified the card networks and provided information to support an investigation by law enforcement.

Over the general time frame of February 18, 2019 to September 27, 2019, malware was installed on certain point-of-sale devices in Islands restaurants that were used for payment card transactions. The time frames involved vary by restaurant. Not all restaurants were involved, and for some restaurants some but not all devices were involved. And at many of the restaurants involved, cards were not successfully obtained during certain weeks in March 2019. So, it is possible that not every card used at a restaurant during the time frame involved was found by the malware.

The malware has been removed from all locations. A list of the specific restaurants involved and their respective time frames can be found by clicking the Locations tab above.

What Information Was Involved?

The malware was designed to look for data read from the magnetic stripe of a payment card as it was being routed through the system. Data in the magnetic stripe includes the cardholder name, card number, expiration date, and internal verification code. In some instances, the malware only identified the portion of the magnetic stripe that contained payment card information without the cardholder name.

What We Are Doing.

Islands values the relationship we have with our guests and understands the importance of protecting payment card information. It is our policy to regularly update and strengthen our systems and processes to help prevent unauthorized access. Upon learning of this incident, Islands quickly took measures to contain the incident and remove the malware. As part of our ongoing commitment to protecting guest information and privacy, we are working with leading partners in cybersecurity to strengthen and enhance payment card security and the security of systems as we go forward. Islands will continue to work with law enforcement and the payment card networks.

What You Can Do.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued your card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you can take.

For More Information.

We regret that this incident occurred and apologize for any inconvenience. If you have any questions, please call 833-935-1380 from 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

PRESS RELEASE

FOR IMMEDIATE RELEASE

Champagne French Bakery Café Announces Payment Card Incident

CARLSBAD, CA – December 19, 2019 – Champagne French Bakery Café was alerted to a potential payment card issue, immediately started an investigation, and took steps to end unauthorized access to our payment card network. A leading computer forensic firm was engaged, and a thorough investigation was conducted to determine what occurred and what restaurant locations and time frames were involved. Champagne Bakery notified the card networks and provided information to support an investigation by law enforcement.

Over the general time frame of February 18, 2019 to September 27, 2019, malware was installed on certain point-of-sale devices in our restaurants that were used for payment card transactions. The time frames involved vary by restaurant. And for the majority of the restaurants involved, cards were not successfully obtained during certain weeks in March 2019. The malware was designed to look for data read from the magnetic stripe of a payment card as it was being routed through the system. Data in the magnetic stripe includes the cardholder name, card number, expiration date, and internal verification code. In some instances, the malware only identified the portion of the magnetic stripe that contained payment card information without the cardholder name.

Lists of the restaurants involved and their respective time frames are available at:

www.champagnebakery.com/paymentcardnotification

This site also provides information about the incident and additional steps customers may take.

Champagne Bakery quickly took measures to contain the incident, remove the malware, and has been working to implement measures to further enhance payment card security. It is always advisable to remain vigilant to the possibility of fraud by reviewing payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued your card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card.

For more information regarding this incident, customers may visit the sites listed above or call 833-935-1383 Monday through Friday between the hours of 6:00 a.m. to 6:00 p.m. Pacific Time.

CHAMPAGNE FRENCH BAKERY CAFE SUBSTITUE NOTICE

Notice of Data Breach

What Happened?

Champagne French Bakery Café was alerted to a potential payment card issue, immediately started an investigation, and took steps to end unauthorized access to our payment card network. A leading computer forensic firm was engaged, and a thorough investigation was conducted to determine what occurred and what restaurant locations and time frames were involved. Champagne Bakery notified the card networks and provided information to support an investigation by law enforcement.

Over the general time frame of February 18, 2019 to September 27, 2019, malware was installed on certain point-of-sale devices in Champagne Bakery restaurants that were used for payment card transactions. The time frames involved vary by restaurant. And for the majority of the restaurants involved, cards were not successfully obtained during certain weeks in March 2019. The malware has been removed from all locations. A list of the specific restaurants involved and their respective time frames can be found by clicking the Locations tab above.

What Information Was Involved?

The malware was designed to look for data read from the magnetic stripe of a payment card as it was being routed through the system. Data in the magnetic stripe includes the cardholder name, card number, expiration date, and internal verification code. In some instances, the malware only identified the portion of the magnetic stripe that contained payment card information without the cardholder name.

What We Are Doing.

Champagne Bakery values the relationship we have with our guests and understands the importance of protecting payment card information. It is our policy to regularly update and strengthen our systems and processes to help prevent unauthorized access. Upon learning of this incident, Champagne Bakery quickly took measures to contain the incident and remove the malware. As part of our ongoing commitment to protecting guest information and privacy, we are working with leading partners in cybersecurity to strengthen and enhance payment card security and the security of systems as we go forward. Champagne Bakery will continue to work with law enforcement and the payment card networks.

What You Can Do.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to the bank that issued your card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you can take.

For More Information.

We regret that this incident occurred and apologize for any inconvenience. If you have any questions, please call 833-935-1383 from 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft