

Media Contact:
Angela Johnson
The Krystal Company
+1 (770) 351.4564
angela.johnson@krystal.com



Notice of Potential Payment Card Incident

ATLANTA — Oct. 24, 2019 — The Krystal Company would like to advise guests that our company is actively investigating a security incident that involves one of the payment processing systems that services some of our restaurants.

Our company has retained a leading forensics firm and is conducting an investigation to determine the extent to which information in Krystal's systems may have been impacted. We are cooperating with law enforcement and have also notified the payment card networks of the investigation.

Although our investigation is in its early stages, we have learned that the security incident may have involved payment cards processed by a payment processing system used at certain restaurants between July through September 2019. Krystal uses multiple payment processing systems and, as a result, not all Krystal restaurants have been impacted by this incident. We have already taken steps to contain and remediate the incident. We are working hard to determine the specific locations and dates for each restaurant involved in the attack. To date, our investigation has determined that about a third of our restaurants are not impacted.

To ensure guests have the latest information, we have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates about this incident. Currently, we have posted on our website a list of restaurant locations that may be impacted. Guests may also call our call center at 1-800-457-9782, which is open 24 hours, 7-days-a-week. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Krystal is committed to protecting the privacy and security of our customers and will continue to take quick action. While our investigation continues, we would like to remind all of our guests to be vigilant and that it is always good practice to review their payment card statements regularly and report any unusual or unauthorized purchases to their financial institution.

About The Krystal Company

Founded in Chattanooga, Tennessee, in 1932, The Krystal Company is the original quick-service restaurant chain in the South and was selected to [USA Today's 2019 Top-10 Best Regional Fast Food List](#). Krystal hamburgers are still served fresh and hot off the grill on the iconic square bun at approximately 320 restaurants in 10 states. Krystal's Atlanta-based Restaurant Support Center serves a team of 7,500 employees. For more information, visit krystal.com.



NOTICE OF POTENTIAL PAYMENT CARD INCIDENT

[Notice](#)[Locations](#)

The Krystal Company would like to advise guests that our company is actively investigating a security incident that involves one of the payment processing systems that services some of our restaurants.

Our company has retained a leading forensics firm and is conducting an investigation to determine the extent to which information in Krystal's systems may have been impacted. We are cooperating with law enforcement and have also notified the payment card networks of the investigation.

Although our investigation is in its early stages, we have learned that the security incident may have involved payment cards processed by a payment processing system used at certain restaurants between July through September 2019. Krystal uses multiple payment processing systems and, as a result, not all Krystal restaurants have been impacted by this incident. We have already taken steps to contain and remediate the incident. We are working hard to determine the specific locations and dates for each restaurant involved in the attack. To date, our investigation has determined that about a third of our restaurants that are not impacted.

To ensure guests have the latest information, we have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates about this incident. Currently, we have posted on our website a list of restaurant locations that may be impacted. Guests may also call our call center at 1-800-457-9782, which is open 24 hours, 7 days-a-week. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Krystal is committed to protecting the privacy and security of our customers and will continue to take quick action. While our investigation continues, we would like to remind all of our guests to be vigilant and that it is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

FREQUENTLY ASKED QUESTIONS

Q: What happened?

A: The Krystal Company is actively investigating a security incident that involves one of the payment processing systems that services some of our restaurants. We are cooperating with law enforcement and have also notified the payment cards networks about the investigation.

Although our investigation is in its early stages, we have learned that the security incident may have involved payment cards processed by a payment processing system used at certain restaurants between July through September 2019. Krystal uses multiple payment processing systems, and as a result, not all Krystal restaurants have been impacted by this incident. We have already taken steps to contain and remediate the incident. We are working hard to determine the specific locations and dates for each restaurant involved in the attack. To date, our investigation has determined that

about a third of our restaurants are not impacted. To ensure guests have the latest information, we have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates about this incident.

Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted. Krystal is committed to protecting the privacy and security of our customers and will continue to take quick action.

Q: When did the incident occur?

A: Although our investigation is in its early stages, we believe that payment cards used at certain restaurants between July through September 2019 may have been impacted. We are working hard to determine specific locations and dates for each restaurant involved in the attack. Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Q: What locations may have been involved/affected?

A: Our investigation is ongoing. We are still determining specific locations and dates for each restaurant involved in the attack.

Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Q: Has this attack been contained?

A: Yes. We have already taken steps to contain and remediate the incident. As part of our ongoing commitment to protecting guest information and privacy, we will work with leading partners in cybersecurity to take steps to strengthen and enhance the security of our systems as we go forward.

Q: What kind of information or data may have been affected?

A: We believe the security incident may have impacted payment cards, including debit and credit card numbers, used at certain restaurants between July through September 2019.

Q: How can I tell if my payment card/credit card may have been affected?

A: We believe the security incident involves one of the payment processing systems that services some of our restaurants. The incident may have impacted payment cards, including debit and credit cards, used at certain restaurants between July through September 2019. We are working hard to determine specific locations and dates for each restaurant involved in the attack. Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted. While our investigation continues, Krystal would like to remind guests that it is always good practice to review their payment card statements regularly and report any unusual or unauthorized purchases to their financial institution.

Q: Are you working with law enforcement?

A: Yes. We are cooperating with law enforcement.

Q: Do I need to cancel or replace my debit/credit card? Do I need to notify my bank or card company?

A: It is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

Q: Is it safe for guests to shop/use credit or debit cards at Krystal restaurants?

A: Yes. We have already taken steps to contain and remediate the incident.

Q: How can I get more information?

A: We have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates for guests about this incident. Please direct any guests to our website or call center if they have questions.

1455 Lincoln Pkwy, Ste 600
Dunwoody, GA 30346
770-351-4500

Menu

Offers

Nutrition Facts

Gift Cards

Find a Store

Browse All

Careers

Franchising

Contact Us

Newsroom

COVID-19 Statement

Media Contact:
Angela Johnson
The Krystal Company
+1 (770) 351.4564
angela.johnson@krystal.com



Notice of Potential Payment Card Incident

ATLANTA — Oct. 24, 2019 — The Krystal Company would like to advise guests that our company is actively investigating a security incident that involves one of the payment processing systems that services some of our restaurants.

Our company has retained a leading forensics firm and is conducting an investigation to determine the extent to which information in Krystal's systems may have been impacted. We are cooperating with law enforcement and have also notified the payment card networks of the investigation.

Although our investigation is in its early stages, we have learned that the security incident may have involved payment cards processed by a payment processing system used at certain restaurants between July through September 2019. Krystal uses multiple payment processing systems and, as a result, not all Krystal restaurants have been impacted by this incident. We have already taken steps to contain and remediate the incident. We are working hard to determine the specific locations and dates for each restaurant involved in the attack. To date, our investigation has determined that about a third of our restaurants are not impacted.

To ensure guests have the latest information, we have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates about this incident. Currently, we have posted on our website a list of restaurant locations that may be impacted. Guests may also call our call center at 1-800-457-9782, which is open 24 hours, 7-days-a-week. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Krystal is committed to protecting the privacy and security of our customers and will continue to take quick action. While our investigation continues, we would like to remind all of our guests to be vigilant and that it is always good practice to review their payment card statements regularly and report any unusual or unauthorized purchases to their financial institution.

About The Krystal Company

Founded in Chattanooga, Tennessee, in 1932, The Krystal Company is the original quick-service restaurant chain in the South and was selected to [USA Today's 2019 Top-10 Best Regional Fast Food List](#). Krystal hamburgers are still served fresh and hot off the grill on the iconic square bun at approximately 320 restaurants in 10 states. Krystal's Atlanta-based Restaurant Support Center serves a team of 7,500 employees. For more information, visit krystal.com.



NOTICE OF POTENTIAL PAYMENT CARD INCIDENT

[Notice](#)[Locations](#)

The Krystal Company would like to advise guests that our company is actively investigating a security incident that involves one of the payment processing systems that services some of our restaurants.

Our company has retained a leading forensics firm and is conducting an investigation to determine the extent to which information in Krystal's systems may have been impacted. We are cooperating with law enforcement and have also notified the payment card networks of the investigation.

Although our investigation is in its early stages, we have learned that the security incident may have involved payment cards processed by a payment processing system used at certain restaurants between July through September 2019. Krystal uses multiple payment processing systems and, as a result, not all Krystal restaurants have been impacted by this incident. We have already taken steps to contain and remediate the incident. We are working hard to determine the specific locations and dates for each restaurant involved in the attack. To date, our investigation has determined that about a third of our restaurants that are not impacted.

To ensure guests have the latest information, we have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates about this incident. Currently, we have posted on our website a list of restaurant locations that may be impacted. Guests may also call our call center at 1-800-457-9782, which is open 24 hours, 7 days-a-week. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Krystal is committed to protecting the privacy and security of our customers and will continue to take quick action. While our investigation continues, we would like to remind all of our guests to be vigilant and that it is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

FREQUENTLY ASKED QUESTIONS

Q: What happened?

A: The Krystal Company is actively investigating a security incident that involves one of the payment processing systems that services some of our restaurants. We are cooperating with law enforcement and have also notified the payment cards networks about the investigation.

Although our investigation is in its early stages, we have learned that the security incident may have involved payment cards processed by a payment processing system used at certain restaurants between July through September 2019. Krystal uses multiple payment processing systems, and as a result, not all Krystal restaurants have been impacted by this incident. We have already taken steps to contain and remediate the incident. We are working hard to determine the specific locations and dates for each restaurant involved in the attack. To date, our investigation has determined that

about a third of our restaurants are not impacted. To ensure guests have the latest information, we have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates about this incident.

Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted. Krystal is committed to protecting the privacy and security of our customers and will continue to take quick action.

Q: When did the incident occur?

A: Although our investigation is in its early stages, we believe that payment cards used at certain restaurants between July through September 2019 may have been impacted. We are working hard to determine specific locations and dates for each restaurant involved in the attack. Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Q: What locations may have been involved/affected?

A: Our investigation is ongoing. We are still determining specific locations and dates for each restaurant involved in the attack.

Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Q: Has this attack been contained?

A: Yes. We have already taken steps to contain and remediate the incident. As part of our ongoing commitment to protecting guest information and privacy, we will work with leading partners in cybersecurity to take steps to strengthen and enhance the security of our systems as we go forward.

Q: What kind of information or data may have been affected?

A: We believe the security incident may have impacted payment cards, including debit and credit card numbers, used at certain restaurants between July through September 2019.

Q: How can I tell if my payment card/credit card may have been affected?

A: We believe the security incident involves one of the payment processing systems that services some of our restaurants. The incident may have impacted payment cards, including debit and credit cards, used at certain restaurants between July through September 2019. We are working hard to determine specific locations and dates for each restaurant involved in the attack. Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted. While our investigation continues, Krystal would like to remind guests that it is always good practice to review their payment card statements regularly and report any unusual or unauthorized purchases to their financial institution.

Q: Are you working with law enforcement?

A: Yes. We are cooperating with law enforcement.

Q: Do I need to cancel or replace my debit/credit card? Do I need to notify my bank or card company?

A: It is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

Q: Is it safe for guests to shop/use credit or debit cards at Krystal restaurants?

A: Yes. We have already taken steps to contain and remediate the incident.

Q: How can I get more information?

A: We have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates for guests about this incident. Please direct any guests to our website or call center if they have questions.

1455 Lincoln Pkwy, Ste 600
Dunwoody, GA 30346
770-351-4500

Menu

Offers

Nutrition Facts

Gift Cards

Find a Store

Browse All

Careers

Franchising

Contact Us

Newsroom

COVID-19 Statement

NOTICE OF POTENTIAL PAYMENT CARD INCIDENT

[Notice](#)[Locations](#)

Although our investigation is in its early stages, we have learned that the security incident may have involved payment cards processed by a payment processing system used at certain restaurants between July through September 2019. Krystal is working hard to determine the specific locations and dates for each restaurant involved in the attack. Below is a list of restaurant locations that may be impacted and can be searched using the look-up tool below. If you do not see a specific restaurant location when searching this tool, that restaurant has not been identified as potentially impacted.

Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

PLEASE SELECT THE STATE THAT YOUR PAYMENT CARD WAS USED IN

Please select a state

FREQUENTLY ASKED QUESTIONS

Q: What happened?

A: The Krystal Company is actively investigating a security incident that involves one of the payment processing systems that services some of our restaurants. We are cooperating with law enforcement and have also notified the payment cards networks about the investigation.

Although our investigation is in its early stages, we have learned that the security incident may have involved payment cards processed by a payment processing system used at certain restaurants between July through September 2019. Krystal uses multiple payment processing systems, and as a result, not all Krystal restaurants have been impacted by this incident. We have already taken steps to contain and remediate the incident. We are working hard to determine the

specific locations and dates for each restaurant involved in the attack. To date, our investigation has determined that about a third of our restaurants are not impacted. To ensure guests have the latest information, we have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates about this incident.

Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted. Krystal is committed to protecting the privacy and security of our customers and will continue to take quick action.

Q: When did the incident occur?

A: Although our investigation is in its early stages, we believe that payment cards used at certain restaurants between July through September 2019 may have been impacted. We are working hard to determine specific locations and dates for each restaurant involved in the attack. Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Q: What locations may have been involved/affected?

A: Our investigation is ongoing. We are still determining specific locations and dates for each restaurant involved in the attack.

Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted.

Q: Has this attack been contained?

A: Yes. We have already taken steps to contain and remediate the incident. As part of our ongoing commitment to protecting guest information and privacy, we will work with leading partners in cybersecurity to take steps to strengthen and enhance the security of our systems as we go forward.

Q: What kind of information or data may have been affected?

A: We believe the security incident may have impacted payment cards, including debit and credit card numbers, used at certain restaurants between July through September 2019.

Q: How can I tell if my payment card/credit card may have been affected?

A: We believe the security incident involves one of the payment processing systems that services some of our restaurants. The incident may have impacted payment cards, including debit and credit cards, used at certain restaurants between July through September 2019. We are working hard to determine specific locations and dates for each restaurant involved in the attack. Currently, we have posted on our website a list of restaurant locations that may be impacted. Krystal will provide updates to guests once we have completed our investigation and know more about payment cards that may have been impacted. While our investigation continues, Krystal would like to remind guests that it is always good practice to review their payment card statements regularly and report any unusual or unauthorized purchases to their financial institution.

Q: Are you working with law enforcement?

A: Yes. We are cooperating with law enforcement.

Q: Do I need to cancel or replace my debit/credit card? Do I need to notify my bank or card company?

A: It is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

Q: Is it safe for guests to shop/use credit or debit cards at Krystal restaurants?

A: Yes. We have already taken steps to contain and remediate the incident.

Q: How can I get more information?

A: We have set up a dedicated page on our website – www.krystal.com/security – where we will post information and updates for guests about this incident. Please direct any guests to our website or call center if they have questions.

1455 Lincoln Pkwy, Ste 600
Dunwoody, GA 30346
770-351-4500

Menu

Offers

Nutrition Facts

Gift Cards

Find a Store

Browse All

Careers

Franchising

Contact Us

Newsroom

COVID-19 Statement

Media Contact:
Angela Johnson
The Krystal Company
+1 (770) 351.4564
angela.johnson@krystal.com



The Krystal Company Updates Guests on Payment Card Security Incident *Company Completes Investigation and Updates Notice*

ATLANTA — March 19, 2020 — The Krystal Company is advising guests that we have completed our investigation into the security incident previously announced on October 24, 2019 involving one of the payment processing systems that services some of our restaurants. We have updated the dedicated page on our website – <http://krystal.com/security/> – to further explain the incident and provide guidance on what our guests can do to protect their personal information, if they have not already undertaken steps in response to our prior announcement.

Our investigation identified suspicious cyber-related activity in our environment and the presence of malware on certain point of sale terminals associated with one of our payment processing systems. This malware was designed to copy payment card information from cards swiped on an infected point of sale terminal. Based on our investigation, the unauthorized access to payment card information for the impacted payment processing system generally occurred from July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. We have posted on our website a list of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location.

We remind all of our guests to be vigilant and that it is always good practice to review their payment card statements regularly and report any unusual or unauthorized purchases to their financial institution. Guests with additional questions may also call our call center at 1-800-457-9782, which is open 24 hours, 7-days-a-week.

Krystal is committed to ensuring that the personal information in our care is protected, and we sincerely regret any inconvenience or concern this incident may cause. We are continuing to cooperate with law enforcement and the payment card brands concerning the incident, and we will continue to take steps to strengthen and enhance the security of our systems as we move forward.



About The Krystal Company

Founded in Chattanooga, Tennessee, in 1932, The Krystal Company is the original quick-service restaurant chain in the South and was selected to [USA Today's 2019 Top-10 Best Regional Fast Food List](#). Krystal hamburgers are still served fresh and hot off the grill on the iconic square bun at 300 restaurants in 10 states. Krystal's Atlanta-based Restaurant Support Center serves a team of over 6,000 employees. For more information, visit krystal.com.

NOTICE OF SECURITY INCIDENT

[Notice](#)[Locations](#)

At The Krystal Company (“Krystal”), protecting the security of the information in our possession is a responsibility we take very seriously. On Friday, September 27, 2019, Krystal received an alert about a criminal threat actor that has been targeting the U.S. retail, restaurant, and hospitality sectors. Upon receiving this alert, Krystal immediately launched an investigation and retained a leading forensics firm to conduct a comprehensive forensic review.

During our investigation, Krystal identified suspicious cyber-related activity in our environment and the presence of malware on certain point of sale terminals associated with one of our payment processing systems. Krystal promptly took steps to stop the intrusion and the unauthorized access, remove the malware, and remediate the attack. We also promptly notified the payment card brands concerning the suspicious activity and cooperated closely with law enforcement. Though we had not yet completed our investigation or determined the scope of impact, we notified our guests on October 24, 2019 that we were investigating a security incident that involved one of our payment processing systems and identified the restaurants that may have been impacted over the relevant timeframe. As reported in our initial communication, Krystal uses multiple payment processing systems, and therefore, not all Krystal restaurants were impacted by this incident.

We have now completed our investigation into the incident. This site further explains the incident and provides guidance below on what you can do to protect your personal information.

What Happened

Our investigation identified suspicious cyber-related activity in our environment and the presence of malware on certain point of sale terminals associated with one of our payment processing systems. This malware was designed to copy payment card information from cards swiped on an infected point of sale terminal. Based on our investigation, the unauthorized access to payment card information for the impacted payment processing system generally occurred from July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. We have posted [a list](#) of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location. Customers can find this information under the “Locations” tab at the top of this page.

We believe the security incident impacted only payment card information, and specifically the track data read from the magnetic stripe of a payment card. This information may include cardholder names, primary account numbers, credit card expiration dates, and credit card verification codes.

What You Can Do

Please see the “Identity Theft Prevention Tips” below. This information provides additional steps you can take, including how to obtain a free copy of your credit report and place a fraud alert and/or credit freeze on your credit report. In addition, Krystal would like to remind all of our guests to be vigilant and that it is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

For More Information

Krystal is committed to ensuring that your personal information is protected, and we sincerely regret any inconvenience or concern this incident may cause. We are continuing to cooperate with law enforcement and the payment card brands concerning the incident, and we will continue to take steps to strengthen and enhance the security of our systems as we move forward. If you have additional questions, please call our dedicated call center at 1-800-457-9782, which is open 24 hours, 7 days-a-week.

Identity Theft Prevention Tips

Credit Report Monitoring

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at www.annualcreditreport.com, calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax

PO Box 740241 Atlanta, GA 30374

www.equifax.com

888-766-0008

Experian

PO Box 9554

Allen, TX 75013

www.experian.com

888-397-3742

TransUnion

PO Box 2000

Chester, PA 19016

www.transunion.com

800-680-7289

If you suspect you are the victim of identity theft, you have the right to obtain a police report and should contact the proper law enforcement authorities, including local law enforcement. You should also consider contacting your state attorney general (www.naag.org/naag/attorneys-general/whos-my-ag.php) and the Federal Trade Commission and may obtain information from these sources about preventing identity theft:

Federal Trade Commission (FTC)

Bureau of Consumer Protection

600 Pennsylvania Avenue NW

Washington, DC 20580

1-877-IDTHEFT (438-4338)

www.ftc.gov/idtheft

Placing a Security Freeze

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies. You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

<https://www.equifax.com/personal/credit-report-services/>

<https://www.experian.com/freeze/center.html>

<https://www.transunion.com/credit-freeze>

Placing a Fraud Alert

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

State Information

NORTH CAROLINA RESIDENTS

You may obtain information about avoiding identity theft at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
919-716-6400
www.ncdoj.gov

SOUTH CAROLINA RESIDENTS

You may seek additional help from the Identity Theft Unit at:

Office of the Attorney General
Consumer Protection Division
Department of Consumer Affairs
P.O. Box 5757
Columbia, SC 29250
803-734-4200
<https://consumer.sc.gov/identity-theft-unit>

FREQUENTLY ASKED QUESTIONS

Q: What happened?

A: Our investigation identified suspicious cyber-related activity in our environment and the presence of malware on certain of our point of sale terminals associated with one of our payment processing systems. This malware was designed to copy payment card information from cards swiped on an infected point of sale terminal. Based on our investigation, the unauthorized access to payment card information for the impacted payment processing system generally occurred from July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. We have posted on our website **a list** of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location.

Q: When did the incident occur?

A: Based on our investigation, the unauthorized access to payment card information for the impacted payment processing system generally occurred from July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. We have posted on our website **a list** of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location.

Q: What locations may have been involved/affected?

A: We have posted on our website **a list** of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location.

Q: Has this attack been contained?

A: Yes. Krystal promptly took steps to stop the intrusion and unauthorized access, remove the malware, and remediate the attack. We also promptly notified the payment card brands concerning the suspicious activity and cooperated closely with law enforcement. As part of our ongoing commitment to protecting guest information and privacy, we are working with leading partners in cybersecurity to take steps to strengthen and enhance the security of our systems as we go forward.

Q: What kind of information or data may have been affected?

A: We believe the security incident impacted only payment card information, and specifically the track data read from the magnetic stripe of a payment card. This information may include cardholder names, primary account numbers, credit card expiration dates, and credit card verification codes.

Q: How can I tell if my payment card/credit card may have been affected?

A: Based on our investigation, the unauthorized access to payment card information for the impacted payment processing system generally occurred from July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. We have posted on our website **a list** of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location. Krystal would like to remind guests that it is always good practice to review their payment card statements regularly and report any unusual or unauthorized purchases to their financial institution.

Q: Are you working with law enforcement?

A: Yes. We are cooperating closely with law enforcement.

Q: Do I need to cancel or replace my debit/credit card? Do I need to notify my bank or card company?

A: It is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

Q: Is it safe for guests to shop/use credit or debit cards at Krystal restaurants?

A: Yes. We have stopped the intrusion and unauthorized access, removed the malware, and remediated the attack. Krystal is continuing to cooperate with law enforcement and the payment card brands concerning the incident and will continue to take steps to strengthen and enhance the security of its systems as Krystal moves forward.

Q: How can I get more information?

A: We have set up a dedicated page on our website – www.krystal.com/security – where we have posted information and updates for guests about this incident, as well as guidance on what you can do to protect your personal information. If you have additional questions, please call our dedicated call center at 1-800-457-9782, which is open 24 hours, 7 days-a-week.

1455 Lincoln Pkwy, Ste 600
Dunwoody, GA 30346
770-351-4500

Menu
Offers
Nutrition Facts
Gift Cards

Find a Store
Browse All
Careers
Franchising

Contact Us
Newsroom
COVID-19 Statement

NOTICE OF SECURITY INCIDENT

[Notice](#)[Locations](#)

Based on our investigation, the security incident involved payment cards processed by a payment processing system used at certain restaurants between approximately July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. Below is [a list](#) of restaurant locations that may be impacted and can be searched using the look-up tool below. If you do not see a specific restaurant location when searching this tool, that restaurant has not been identified as potentially impacted.

PLEASE SELECT THE STATE THAT YOUR PAYMENT CARD WAS USED IN

Please select a state

FREQUENTLY ASKED QUESTIONS

Q: What happened?

A: Our investigation identified suspicious cyber-related activity in our environment and the presence of malware on certain of our point of sale terminals associated with one of our payment processing systems. This malware was designed to copy payment card information from cards swiped on an infected point of sale terminal. Based on our investigation, the unauthorized access to payment card information for the impacted payment processing system generally occurred from July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. We have posted on our website [a list](#) of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location.

Q: When did the incident occur?

A: Based on our investigation, the unauthorized access to payment card information for the impacted payment processing system generally occurred from July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. We have posted on our website [a list](#) of the restaurant locations involved in the incident and the

respective timeframes of impact, which vary by location.

Q: What locations may have been involved/affected?

A: We have posted on our website **a list** of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location.

Q: Has this attack been contained?

A: Yes. Krystal promptly took steps to stop the intrusion and unauthorized access, remove the malware, and remediate the attack. We also promptly notified the payment card brands concerning the suspicious activity and cooperated closely with law enforcement. As part of our ongoing commitment to protecting guest information and privacy, we are working with leading partners in cybersecurity to take steps to strengthen and enhance the security of our systems as we go forward.

Q: What kind of information or data may have been affected?

A: We believe the security incident impacted only payment card information, and specifically the track data read from the magnetic stripe of a payment card. This information may include cardholder names, primary account numbers, credit card expiration dates, and credit card verification codes.

Q: How can I tell if my payment card/credit card may have been affected?

A: Based on our investigation, the unauthorized access to payment card information for the impacted payment processing system generally occurred from July 2, 2019 through September 27, 2019, with some stores impacted over a shorter timeframe. We have posted on our website **a list** of the restaurant locations involved in the incident and the respective timeframes of impact, which vary by location. Krystal would like to remind guests that it is always good practice to review their payment card statements regularly and report any unusual or unauthorized purchases to their financial institution.

Q: Are you working with law enforcement?

A: Yes. We are cooperating closely with law enforcement.

Q: Do I need to cancel or replace my debit/credit card? Do I need to notify my bank or card company?

A: It is always good practice to review your payment card statements regularly and report any unusual or unauthorized purchases to your financial institution.

Q: Is it safe for guests to shop/use credit or debit cards at Krystal restaurants?

A: Yes. We have stopped the intrusion and unauthorized access, removed the malware, and remediated the attack. Krystal is continuing to cooperate with law enforcement and the payment card brands concerning the incident and will continue to take steps to strengthen and enhance the security of its systems as Krystal moves forward.

Q: How can I get more information?

A: We have set up a dedicated page on our website – www.krystal.com/security – where we have posted information and updates for guests about this incident, as well as guidance on what you can do to protect your personal information. If you have additional questions, please call our dedicated call center at 1-800-457-9782, which is open 24 hours, 7 days-a-week.

1455 Lincoln Pkwy, Ste 600
Dunwoody, GA 30346
770-351-4500

Menu

Offers

Nutrition Facts

Gift Cards

Find a Store

Browse All

Careers

Franchising

Contact Us

Newsroom

COVID-19 Statement

© 2020 The Krystal Company. All rights reserved.

[Privacy Policy](#)