SAMPLE WEBSITE NOTIFICATION

NOTICE OF DATA BREACH

July 19, 2016

Cicis values its customers and respects the privacy of your information. As a precautionary measure, we want to inform you that your personal information may have been compromised as a result of a data breach that impacted certain of Cicis restaurant locations. Cicis regrets any inconvenience this may have caused.

WHAT HAPPENED

While this matter is still under investigation, we wish to report what we currently know. In early March of 2016, we received notice from several of our restaurant locations that their Point of Sale (POS) systems were not working properly. Our POS Vendor began an investigation to assess the problem and initiated heightened security measures. When the POS Vendor found malware on the POS software at some Cicis restaurants, we immediately began a restaurant by restaurant data security review and remediation. We also retained a third party cyber security firm to perform a forensic analysis to determine what, if any, information might have been compromised and to verify that all threats have been eliminated. The forensic firm reported its findings on July 19, 2016 confirming that a malicious software program had been introduced by a hacker to the POS system used by some Cicis restaurant locations. The threat of that malware to our restaurants has been eliminated.

WHAT INFORMATION WAS INVOLVED

The report revealed that payment card information may have been compromised from payment cards used at some Cicis restaurants. The vast majority of intrusions began in March of 2016 and the threats were eliminated on a store by store basis through July of 2016. A smaller percentage of affected restaurants had intrusions dating back to 2015. While we believe most of the breaches were remedied within a few weeks of the intrusion, out of an abundance of caution we are not declaring some restaurants as threat-free until they were reviewed by our forensic analyst this month. The following link contains a list of all affected restaurant locations and the dates of potential vulnerability. Link to list of impacted locations. Not all payment cards used at the affected restaurant locations were compromised; however, some information from some payment cards used in such locations may have been accessed by the malware. No other customer information was compromised.

WHAT WE ARE DOING

As part of our response to this incident, we have notified law enforcement and the state agencies as required by the laws of the jurisdictions in which our restaurants are located, and we will continue to assist with their investigation. The payment card networks have also been informed so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards

used during the timeframe in which cards may have been compromised. Cicis continues to monitor and upgrade our systems to keep your information as secure as possible.

WHAT YOU CAN DO

If you used a payment card during the timeframe listed above at an affected restaurant, you should pay particular attention to your payment card statements for unauthorized activity. Any unauthorized activity should be immediately reported to your card issuer because card payment rules generally provide that cardholders are not responsible for fraudulent transactions that are promptly reported.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

CARD STATEMENT AND CREDIT REPORT MONITORING

We recommend that you protect against payment card fraud and identity theft by carefully monitoring your card statements and by reviewing 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	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

If you find evidence that your payment card data has been misused or that your identity has been stolen, 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. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

FRAUD ALERT

You may also want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible

fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. If you place a fraud alert with any of the three credit reporting agencies, that agency will inform the other two. There are two types of fraud alerts: an Initial Security Alert, which lasts 90 days, and an Extended Fraud Victim Alert, which lasts up to seven years. You should work with the credit reporting agency to select the alert most appropriate for you. If you select an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

SECURITY FREEZE

In some US states, you have the right to put a security freeze on your credit file. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

OBTAIN ADDITIONAL INFORMATION

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

If you are a NORTH CAROLINA resident: You may also wish to review information provided by the North Carolina Attorney General's Office on how to avoid identity theft. Their website address is www.ncdoj.gov. Their toll-free number is 1-877-566-7226. Their mailing address is North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.

ATTACHMENT 2

On Letterhead

Email to Loyalty Club Members

Date

Dear [NAME]

Loyal guests like you are our first priority at Cicis, so we are contacting you directly as a precautionary measure to inform you that we recently received confirmation that hackers gained access to the payment card systems at some Cicis locations, including one or more you may have visited.

We have taken steps to fix the problem, remove the detected malware and have added safety measures to help protect your payment card information from these sophisticated cyber criminals.

Our loyalty program records show that you visited a Cicis restaurant during the timeframe the restaurant's payment systems may have been compromised. If you used a payment card during your visit, it is possible that some of your payment card data was compromised in the attack. We suggest that you pay particular attention to your payment card statements to identify unauthorized or suspicious charges. Any unauthorized charges should be immediately reported to your card issuer.

Please be assured that we are working with the proper authorities in their investigations and have informed payment card networks so they can work with banks to monitor for fraudulent activity. Additional information on how you can protect yourself is available at www.cicis.com/news and on a dedicated, toll-free Privacy Line, (877) 220-1388. Provide reference number 8771062016.

Thank you for being a loyal Cicis customer.

Sincerely,

Darin Harris
Cicis Chief Executive Officer

ATTACHMENT 3

SAMPLE WEBSITE NOTIFICATION

NOTICE OF DATA BREACH

July 19, 2016

Cicis values its customers and respects the privacy of your information. As a precautionary measure, we want to inform you that your personal information may have been compromised as a result of a data breach that impacted certain of Cicis restaurant locations. Cicis regrets any inconvenience this may have caused.

WHAT HAPPENED

While this matter is still under investigation, we wish to report what we currently know. In early March of 2016, we received notice from several of our restaurant locations that their Point of Sale (POS) systems were not working properly. Our POS Vendor began an investigation to assess the problem and initiated heightened security measures. When the POS Vendor found malware on the POS software at some Cicis restaurants, we immediately began a restaurant by restaurant data security review and remediation. We also retained a third party cyber security firm to perform a forensic analysis to determine what, if any, information might have been compromised and to verify that all threats have been eliminated. The forensic firm reported its findings on July 19, 2016 confirming that a malicious software program had been introduced by a hacker to the POS system used by some Cicis restaurant locations. The threat of that malware to our restaurants has been eliminated.

WHAT INFORMATION WAS INVOLVED

The report revealed that payment card information may have been compromised from payment cards used at some Cicis restaurants. The vast majority of intrusions began in March of 2016 and the threats were eliminated on a store by store basis through July of 2016. A smaller percentage of affected restaurants had intrusions dating back to 2015. While we believe most of the breaches were remedied within a few weeks of the intrusion, out of an abundance of caution we are not declaring some restaurants as threat-free until they were reviewed by our forensic analyst this month. The following link contains a list of all affected restaurant locations and the dates of potential vulnerability. Link to list of impacted locations. Not all payment cards used at the affected restaurant locations were compromised; however, some information from some payment cards used in such locations may have been accessed by the malware. No other customer information was compromised.

WHAT WE ARE DOING

As part of our response to this incident, we have notified law enforcement and the state agencies as required by the laws of the jurisdictions in which our restaurants are located, and we will continue to assist with their investigation. The payment card networks have also been informed so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards

SAMPLE WEBSITE NOTIFICATION

used during the timeframe in which cards may have been compromised. Cicis continues to monitor and upgrade our systems to keep your information as secure as possible.

WHAT YOU CAN DO

If you used a payment card during the timeframe listed above at an affected restaurant, you should pay particular attention to your payment card statements for unauthorized activity. Any unauthorized activity should be immediately reported to your card issuer because card payment rules generally provide that cardholders are not responsible for fraudulent transactions that are promptly reported.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

CARD STATEMENT AND CREDIT REPORT MONITORING

We recommend that you protect against payment card fraud and identity theft by carefully monitoring your card statements and by reviewing 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	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

If you find evidence that your payment card data has been misused or that your identity has been stolen, 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. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

FRAUD ALERT

You may also want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible

SAMPLE WEBSITE NOTIFICATION

fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. If you place a fraud alert with any of the three credit reporting agencies, that agency will inform the other two. There are two types of fraud alerts: an Initial Security Alert, which lasts 90 days, and an Extended Fraud Victim Alert, which lasts up to seven years. You should work with the credit reporting agency to select the alert most appropriate for you. If you select an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

SECURITY FREEZE

In some US states, you have the right to put a security freeze on your credit file. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

OBTAIN ADDITIONAL INFORMATION

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

If you are a NORTH CAROLINA resident: You may also wish to review information provided by the North Carolina Attorney General's Office on how to avoid identity theft. Their website address is www.ncdoj.gov. Their toll-free number is 1-877-566-7226. Their mailing address is North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.

SAMPLE WEBSITE NOTIFICATION

If you are a MARYLAND resident, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.
If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400.

If you are a WEST VIRGINIA resident, you also have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is listed above.

FOR MORE INFORMATION.

We understand that you may have questions about this incident that are not addressed in this notification. If you have additional questions, please call our dedicated assistance line at **(877) 220-1388,** Monday through Friday, 9 a.m. to 7 p.m. EST (Closed on U.S. observed holidays) and provide reference number [redacted] when calling.

cicis
BEYOND PIZZA

CICIS ALERTS CUSTOMERS OF DATA BREACH AT SOME LOCATIONS

Systems have been secured at all restaurants

COPPELL, Texas (July 19, 2016) – Cicis says that an ongoing investigation has revealed that payment systems at a limited number of locations were infected by malware that may have been used to expose guests' payment card information. The malware has been removed, and a complete list of affected restaurants is available here.

The company reports that in early March of 2016, it received reports from several of its restaurant locations that point-of-sale systems were not working properly. The point-of-sale vendor immediately began an investigation to assess the problem and initiated heightened security measures. After malware was found on some point-of-sale systems, the company began a restaurant-by-restaurant review and remediation, and retained a third-party cybersecurity firm, 403 Labs, to perform a forensic analysis.

Additional details of the breach and dates of potential exposure are available at www.cicis.com/news. Cicis has also established a dedicated, toll-free Privacy Line to answer guest questions at 877-220-1388. Callers should use reference numbe[redacted]

"Our guests are our first priority at Cicis, and when we first learned of unusual activity in our system, we took immediate action to investigate, root out and fix the problem, and enact further safety measures," said Cicis CEO Darin Harris. "We want to reassure our guests that all malware has been removed, and we will continue to monitor and improve our systems to protect their payment card information."

The company has notified the proper authorities in each state where stores were affected and will work closely with law enforcement in their investigation into this cybercrime.

The company encourages guests who used payment cards at the affected restaurants during the period of potential exposure to monitor their payment card statements so they can immediately report any unauthorized activity to their card issuer. Additional information on how consumers can protect themselves is available at www.cicis.com/news and on the toll-free Privacy Line.

About Cicis
Coppell, Texas-based Cicis has nearly 450 corporate and franchised buffet-style pizza restaurants in 33 states. For more information about Cicis, visit cicis.com or Facebook.com/cicis.

###

Media Contact: Kristen Kauffman
SPM Communications
817-329-3257
kristen@spmcommunications.com