Skip to main content

Notice of Payment Card Incident

Main Event Entertainment, Inc. values the relationship we have with our customers and takes the security of payment card data very seriously. We are notifying our customers of an incident involving payment card data of some customers who made purchases at certain Main Event centers. This notice explains the incident, measures we have taken, and steps customers may consider taking as well.

We recently received a report from a third party suggesting there may have been unauthorized access to data from payment cards that were used at some Main Event centers. We immediately launched an investigation, and leading cybersecurity firms were engaged to assist.

On April 9, 2020, the investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices for food and beverage purchases and entertainment activities (other than arcade kiosks) at some Main Event centers. The malware searched for payment card track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) as it was being routed through the payment processing systems. The malware was removed, and we have implemented enhanced security measures. In addition, we notified law enforcement and continue to support their investigation.

The focus of the investigation then turned to identifying the Main Event centers potentially involved and the timeframes when data from payment cards used at the locations involved may have been accessed. The investigation determined that not all Main Event centers were involved, and the specific timeframes when card data may have been accessed vary by location over the general timeframe beginning July 19, 2019 through March 16, 2020. There is one location where access to card data may have continued through April 7, 2020. A list of the locations involved and specific timeframes is available here (/page/location-look-up-tool). Payment cards used to make purchases on arcade kiosks in Main Event centers or through our website were not involved.

Of particular note, chip-enabled (EMV) technology was implemented on all POS devices in our food and beverage and entertainment spaces (other than behind the bars) on a rolling basis starting in June 2019. For cards inserted into chip-readers, only card number and expiration date (and not the cardholder name or verification code) were potentially involved. There is no indication that other customer information was accessed.

It is always advisable to review your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer 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 below for information on additional steps you may take.

We regret this incident occurred and sincerely apologize for any inconvenience. If customers have additional questions regarding the incident, you can call 855-917-3472 Monday through Friday between the hours of 8:00 a.m. and 8:00 p.m. CT.

Additional Steps You Can Take

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 free annual 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 (https://www.equifax.com/personal/), 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com (https://www.experian.com/), 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com (https://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 (http://www.ftc.gov/idtheft)

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.
How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013,experian.com (https://www.experian.com/)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016,transunion.com (https://www.transunion.com/)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348,equifax.com (https://www.equifax.com/)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: Main Event's mailing address is 5445 Legacy Drive, Suite 400, Plano, TX 75024. You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us (www.oag.state.md.us)

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore (www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.

- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

 CONTACT US

 CAREERS

 COMPANY EVENTS (/event/corporate)

| GIFTCARDS (/page/giftcard) | FOOD & DRINKS (/eat-drink/dining)

(https://www.cognizant.com/cognizantbusinesscloud/OrderServ)

Notice of Payment Card Incident

NEWS PROVIDED BY
Main Event →
Apr 29, 2020, 16:00 ET

PLANO, Texas, April 29, 2020 /PRNewswire/ -- Main Event Entertainment, Inc. ("Main Event") values the relationship we have with our customers and takes the security of payment card data very seriously. We are notifying our customers of an incident involving payment card data of some customers who made purchases at certain Main Event centers. This notice explains the incident, measures we have taken, and steps customers may consider taking as well.

We recently received a report from a third party suggesting there may have been unauthorized access to data from payment cards that were used at some Main Event centers. We immediately launched an investigation, and leading cybersecurity firms were engaged to assist.

On April 9, 2020, the investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices for food and beverage purchases and entertainment activities (other than arcade kiosks) at some Main Event centers. The malware searched for payment card track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) as it was being routed through the payment processing systems. The malware was removed, and we have implemented enhanced security measures. In addition, we notified law enforcement and continue to support their investigation.

The focus of the investigation then turned to identifying the Main Event centers potentially involved and the timeframes when data from payment cards used at the locations involved may have been accessed. The investigation determined that not all Main Event centers were involved, and the specific timeframes when data from cards used at the centers involved may have been accessed vary by location over the general timeframe beginning July 19, 2019

through March 16, 2020. There is one location where access to card data may have continued through April 7, 2020. A list of the locations involved and specific timeframes is available on our website at https://www.mainevent.com/page/paymentcardincident. Payment cards used to make purchases on arcade kiosks in Main Event centers or through our website were not involved.

Of particular note, chip-enabled (EMV) technology was implemented on our food and beverage self-order kiosks prior to the incident, and this technology was also implemented on POS systems in all entertainment spaces (other than behind the bars) on a rolling basis starting in June 2019. For cards inserted into chip-readers, only card number and expiration date (and not the cardholder name or verification code) were potentially involved. There is no indication that other customer information was accessed.

It is always advisable for customers to review their payment card statements for any unauthorized activity and immediately report any unauthorized charges to their card issuer using the number provided on the back of the payment card.

We regret this incident occurred and sincerely apologize for any inconvenience.

For more information regarding this incident, customers may visit https://www.mainevent.com/page/paymentcardincident.

Media Contact
Email: paymentcardincident@mainevent.com

SOURCE Main Event

Related Links

http://www.mainevent.com