

## Winberie's Oak Park Provides Notice of Data Security Incident

**Oak Park, Illinois, June 9, 2017** – Winberie's Oak Park today said that a recent data security incident at its third-party vendor may have compromised the security of payment information of some guests who used a debit or credit card at its restaurant between October 26, 2016 and January 7, 2017. Guests can safely use their credit and debit cards at Winberie's Oak Park.

**What Happened?** On March 30, 2017, Winberie's Oak Park began investigating some unusual activity reported to the Company by its third-party vendor. Winberie's Oak Park began to work with independent forensic experts to investigate these reports and to identify any signs of compromise on its systems. On April 26, 2017, Winberie's Oak Park confirmed suspicious activity on its computer systems that indicated a potential compromise of guests' debit and credit card data for some debit and credit cards used at its restaurant.

Since that time, Winberie's Oak Park has been working with third-party forensic investigators to determine what happened, what information was affected, protect the security of guest debit and credit cards, confirm the removal of the malware, and implement procedures to prevent any further unauthorized access to guest debit or credit card information. Winberie's Oak Park is working with the United States Secret Service to investigate this incident.

**What Information Was Involved?** Through the ongoing third-party forensic investigations, Winberie's Oak Park confirmed on April 26, 2017 that malware may have stolen credit or debit card data from some credit and debit cards used at Winberie's Oak Park locations between October 26, 2016 and January 7, 2017. The date range differs for each affected Winberie's Oak Park location. The information at risk as a result of this event may include the cardholder's name, card number, expiration date and CVV.

**What We Are Doing.** "Winberie's Oak Park takes the security of our guests' information seriously, and we apologize for the inconvenience this incident has caused our guests," Alan Donatelli, President & COO of Winberie's, said. "We continue to work with third-party forensic investigators and law enforcement officials to ensure the security of our systems, and do all we can on behalf of our guests."

**For More Information.** Winberie's Oak Park has established a dedicated assistance line for individuals seeking additional information regarding this incident. Guests can call **(877) 238-2151**, Monday through Friday, 9 a.m. to 7 p.m. EST (Closed on U.S. observed holidays) and provide reference number **8204060617** when calling.

**What You Can Do.** Winberie's Oak Park encourages all guests to remain vigilant against incidents of identity theft by reviewing their account statements regularly and monitoring their credit reports for suspicious activity. Under U.S. law, a guest over the age of 18 is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. A guest may also contact the three major credit bureaus directly to request a free copy of their credit report.

Winberie's Oak Park encourages guests who believe they may be affected by this incident to take additional action to further protect against possible identity theft or other financial loss. At no charge, a guest can also have these credit bureaus place a "fraud alert" on their file that alerts creditors to take additional steps to verify their identity prior to granting credit in their name. Note, however, that because it tells creditors to follow certain procedures to protect the guest, it may also delay their ability to obtain credit while the agency verifies their identity. As soon as one credit bureau confirms the guest's fraud alert, the others are notified to place fraud alerts on the guest's file. Should the guest wish to place a fraud alert, or should the guest have any questions regarding his or her credit report, the guest can contact any one of the agencies listed below.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19022  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

A guest may also place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a guest's credit report without the consumer's written authorization. However, a guest should be aware that placing a security freeze on their credit report may delay, interfere with, or prevent the timely approval of any requests they make for new loans, credit mortgages, employment, housing, or other services.

If a guest has been a victim of identity theft, and the guest provides the credit reporting agency with a valid police report, it cannot charge the guest to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge a guest a fee to place, temporarily lift, or permanently remove a security freeze. A guest will need to place a security freeze separately with each of the three major credit bureaus listed above if the guest wishes to place the freeze on all of their credit files.

To find out more on how to place a security freeze, a guest can contact the credit reporting agencies using the information below:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
(NY residents please call  
1-800-349-9960)  
[www.freeze.equifax.com](http://www.freeze.equifax.com)

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion  
PO Box 2000  
Chester, PA 19022-2000  
1-888-909-8872  
[www.transunion.com/securityfreeze](http://www.transunion.com/securityfreeze)

A guest can further educate themselves regarding identity theft, fraud alerts, and the steps they can take to protect themselves, by contacting the Federal Trade Commission or their state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov). **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16<sup>th</sup> Floor,

Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. A guest can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.