

**LEWIS
BRISBOIS
BISGAARD
& SMITH LLP**
ATTORNEYS AT LAW

1055 Westlakes Drive, Suite 300
Berwyn, Pennsylvania 19312
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

JAMES E. PRENDERGAST
DIRECT DIAL: 215.977.4058
JIM.PRENDERGAST@LEWISBRISBOIS.COM

May 16, 2014

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Affinity Gaming – Notice of Data Event

Dear Mr. Foster:

We are writing to notify you of a data event that may have compromised the security of certain credit/debit card information. Affinity Gaming, a Nevada corporation with corporate headquarters in Las Vegas, is informing your office of pertinent facts that are known at this time related to an unauthorized intrusion into the system which processes customers' credit/debit card information. This illegal intrusion is believed to have occurred between December 7, 2013 and April 28, 2014 and resulted in unauthorized access by unknown individual(s) to the names and credit/debit card data of some of our customers. Upon discovery of the unauthorized access, Affinity retained independent, third-party computer forensic specialists, Mandiant, to assist with its investigation of, and response to, this incident. Affinity also retained specialized data privacy counsel. The investigation is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Affinity does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

Affinity learned, on April 17, 2014, that credit/debit card information processed on its system may have been accessed and exported by unknown individuals. The payment card data which passed through the servers between December 7, 2013 and April 28, 2014 was exposed to unauthorized individuals. Immediately after first notice of the compromise, Affinity retained computer forensic specialists, Mandiant, to perform an investigation into the compromise. Mandiant determined that unknown individual(s) had unauthorized access to names and credit/debit card data for some of Affinity's customers. Affinity is aware of fraud believed to be related to this compromise.

Mandiant and Affinity have secured the payment card system, and are working closely and continuously with the United States Secret Service and the Federal Bureau of Investigation.

Notice to New Hampshire Residents

Because Affinity does not store credit card data, it does not know the number of affected New Hampshire residents. Affinity first posted notice of this incident on its website on April 24, 2014. While the forensic investigation was still ongoing, Affinity subsequently posted updates regarding the compromise on its website on or about May 5th and May 7th of 2014. Upon determination of the scope of this incident, Affinity posted an additional notice on its website on or about May 16, 2014, in substantially the same form as the sample notice attached to this letter as *Exhibit A*. Affinity also submitted the same notice to state-wide media in the United States on or about May 16, 2014. Affinity promptly notified the credit card companies and the appropriate banks and credit card processing company of the compromise.

Other Steps Taken and To Be Taken

As discussed above, Affinity retained forensic computer experts, as well as legal counsel specializing in data breach response. Affinity is providing information on how to protect against identity theft and fraud. Affinity is also providing written notice of this data event to other state and international regulators, many other media companies, and consumer reporting agencies. Affinity has organized a call center to assist any affected individual with questions.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4058.

Very truly yours,



James E. Prendergast of
LEWIS BRISBOIS BISGAARD & SMITH LLP

JEP:sn
Enclosure

EXHIBIT A

Affinity Gaming Provides Public Notice of Unauthorized IT System Access

Patrons Encouraged to Take Steps to Protect Identity and Financial Information

LAS VEGAS, May 16, 2014 - Affinity Gaming ("Affinity") has confirmed an unauthorized intrusion into the system that processes customer credit and debit cards for non-ATM transactions at its casino and casino resort properties, and is issuing this public notice of the data security incident. Affinity is encouraging individuals who visited its facilities and used their credit or debit cards for hotel, food and beverage, or retail transactions between December 7, 2013, and April 28, 2014, to take steps to protect their identities and financial information. ATM and cash advance transactions were not affected. Affinity takes this matter very seriously, and has established a confidential, toll-free inquiry line to assist its customers.

"Our customers are our top priority and we can assure them we are working tirelessly, using best-in-class experts to protect our IT system and their information," said David Ross, Chief Executive Officer at Affinity. "We deeply regret any inconvenience this incident may cause and are ensuring our customers have the information they need to address any concerns."

On April 17, 2014, Affinity was conducting a security audit of its IT systems, when it identified a possible issue in the system that processes debit and credit card transactions. Affinity immediately initiated a thorough investigation, supported by a top-tier and globally recognized, third-party data forensics expert, Mandiant, which determined the nature and scope of the compromise. Mandiant's and Affinity's teams worked aggressively to fully secure the payment card systems and ensure that customer payments are protected. Affinity promptly and repeatedly posted notices of this incident on its website, in an effort to inform and update customers of its ongoing investigation.

Affinity's investigation, while still continuing, has determined that its system was attacked by hackers, which resulted in a compromise of credit card and debit card information used in non-gaming purchases from individuals who visited its casino and casino resort facilities: Silver Sevens Hotel & Casino in Las Vegas, NV; Rail City Casino in Sparks, NV; Primm Valley Resort & Casino in Primm, NV; Buffalo Bill's Resort & Casino in Primm, NV; Whiskey Pete's Hotel & Casino in Primm, NV; Lakeside Hotel-Casino in Osceola, IA; St. Jo Frontier Casino in St. Joseph, MO; Mark Twain Casino in LaGrange, MO; Golden Gates Casino in Black Hawk, CO; Golden Gulch Casino in Black Hawk, CO; and Mardi Gras Casino in Black Hawk, CO. Credit or debit card data was exposed at these locations for those customers making hotel, food and beverage, and retail purchases with their cards between December 7, 2013 and April 28, 2014.

Affinity encourages its patrons to protect against possible identity theft or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, Affinity customers can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud

alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/bcp/edu/microsites/idtheft/ or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. State Attorneys General may also have advice on preventing identity theft, and instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

The confidential inquiry line established by Affinity is available Monday through Friday, 6:00 a.m. to 6:00 p.m. P.S.T. and can be reached at (877) 238-2179 (U.S. and Canadian residents) or +1 (814) 201-3696 (international residents).

Affinity remains dedicated in its commitment to the security of its customers' information and will continue to evolve and enhance system security in anticipation of new and emerging threats. Affinity is providing website notice of this incident and substitute notice of this incident in the states and territories where its customers reside. Affinity is also working closely with the United States Secret Service and the United States Federal Bureau of Investigation, in order to bring whoever is responsible for this incident to justice. Affinity is notifying gaming regulators, and certain state and international regulators. Affinity has notified the credit card companies and the appropriate banks. Affinity has also undertaken systematic and uncompromising efforts to strengthen the security of its data network, and to identify and implement additional appropriate safeguards.

Media Contact:

Harry Frazier

Email: harry.frazier@fleishman.com

Phone: 202.828.8897