



James E. Prendergast
D: 215.358.5087
jprendergast@nldhlaw.com

518 Township Line Road
Suite 300
Blue Bell, PA 19422
P: 215.358.5100
F: 215.358.5101

December 19, 2013

Via Regular Mail

Attorney General Michael A. Delaney
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. Delaney:

We are writing to notify you of a data event that may have compromised the security of certain credit 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 a suspected illegal intrusion into two of its servers that contained customers' credit card information. This illegal intrusion is believed to have occurred between March 14, 2013 and October 16, 2013 and resulted in unauthorized access by unknown individual(s) to the names and credit card data of some of our customers. When Affinity first learned of the compromise, the intrusion had already been contained. Upon discovery of the unauthorized access, Affinity retained independent, third-party computer forensic specialists, Trustwave, to assist with its investigation of, and response to, this incident. Affinity also retained data privacy counsel, Nelson Levine deLuca & Hamilton, to assist in the notification process and act as Affinity's 'breach coach', to guide Affinity's reporting requirements and responses concerning this event. 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 October 24, 2013, that credit card information processed on its central servers may have been accessed and exported by unknown individuals. The credit card data which passed through the servers between March 14 and October 16, 2013 was potentially exposed to unauthorized individuals. Immediately after first notice of the compromise, Affinity

retained computer forensic specialists Trustwave to perform an investigation into the compromise. Trustwave determined that the compromise had concluded before it began its investigations. Trustwave determined that unknown individual(s) had unauthorized access to names and credit card data for some of Affinity's customers. Affinity is aware of alleged fraud believed to be related to this compromise. Affinity has worked closely and continuously with local and federal law enforcement since the beginning of this investigation

Notice to New Hampshire Residents

Because Affinity does not store credit card data, it does know the number of affected New Hampshire residents. Affinity first posted notice of this incident on its website on November 14, 2013. Affinity will post subsequent notice of the compromise on its website on or about December 20, 2013, in substantially the same form as the sample notice attached to this letter as *Exhibit A*. Affinity will also submit the same notice to state-wide media on or about December 20, 2013. Affinity promptly notified the credit card companies and the appropriate banks and credit card processing company of the compromise.

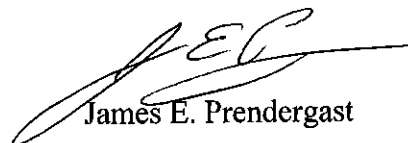
Other Steps Taken and To Be Taken

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 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 215-358-5087.

Sincerely,



James E. Prendergast

cc: Affinity Gaming

Exhibit A

Affinity Gaming Provides Public Notice of Data Security Incident

Gaming Facility Patrons Encouraged to Take Steps to Protect Identity and Financial Information

LAS VEGAS, December 20, 2013 – Affinity Gaming (“Affinity”) has confirmed an unauthorized intrusion into the system that processes customer credit and debit cards for its casinos, and is issuing this public notice of the data security incident and encouraging individuals who visited its gaming facilities between March 14th and October 16th of 2013 to take steps to protect their identities and financial information. Affinity regrets any inconvenience this incident may cause and has established a confidential, toll-free inquiry line to assist its customers.

Affinity has also confirmed an unauthorized intrusion into the system that processes credit and debit cards at its Primm Center Gas Station in Primm, Nevada. This intrusion began on an unknown date and it ended on November 29, 2013.

On October 24, 2013, Affinity was contacted by law enforcement regarding fraudulent charges which may have been linked to a data breach in Affinity’s system. Affinity immediately initiated a thorough investigation, supported by third-party data forensics experts who determined the nature and scope of the compromise, and confirmed that Affinity’s system has been fully secured and that its customer payments are protected. On November 14, 2013, Affinity posted notice of this incident on its website.

Affinity’s investigation, while ongoing, has also determined that its system became infected by malware, which resulted in a compromise of credit card, and debit card, information from individuals who visited its gaming 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 between March 14th and October 16th of 2013.

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, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please 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; 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, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your 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, 8:00 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 steadfast in its commitment to the security of its patrons' information. Affinity is providing website notice of this incident and substitute notice of this incident in the states where its customers reside. Affinity has also provided notice to local law enforcement, the United States Secret Service, the United States Federal Bureau of Investigation, gaming regulators, and to certain state and international regulators. Affinity has notified the credit card companies and the appropriate banks. Affinity is cooperating in the ongoing law enforcement investigation of the incident. Affinity has also taken a number of measures to strengthen the security of our network and it has worked with legal and security vulnerability experts to help identify and implement additional appropriate safeguards.

Media Contact: James E. Prendergast at: jprendergast@nldhlaw.com or at 215-358-5087.