January 31, 2015

New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Blue Sky Casino LLC / Security Incident Involving Credit Card Data

Dear Sir or Madam:

This letter is respectfully submitted to the New Hampshire Attorney General's Office in relation to a security breach involving credit card data, which was experienced by our client, Blue Sky Casino LLC. Blue Sky Casino is the owner of the French Lick Resort in Indiana, which includes the French Lick Springs Hotel, the French Lick Casino, golf courses and the West Baden Springs Hotel. Although your office already received notification of this incident on January 28, 2015, via an email from [redacted] Illinois Assistant Attorney General, we wanted to formalize the notification via this letter in order to ensure full compliance with the state breach notification obligations.

This incident included breach notification letters to 17 residents of New Hampshire.

The Resort initially became aware if this situation on January 13, 2015, via a credit union in Indiana that reported credit card compromises on 28 accounts. The common link appeared to be use of the credit cards at the Resort. The Resort managers and IT security team took immediate steps to evaluate possible intrusion with assistance from their incident response team as well as external legal and IT security/forensics experts.

On January 19th, the IT security/forensics experts identified malware that had been installed on the system on April 22, 2014, and which was activated on April 23, 2014. The IT team was able to neutralize the malware on January 19th, and confirmed on January 21st, that they had neutralized/blocked it from capturing any more credit card data.

The Resort also retained PCI-certified forensics experts to help ensure that its system is protected from security compromises on a go-forward basis, and is working with law enforcement authorities to help identify and prosecute the hackers.

In order to notify all possible affected individuals, the Resort sent notification letters to all 87,975 guests, visitors and employees who were identified from its databases (e.g., hotels, casino, golf course, etc.) during the period that the malware was active, and issued a press release to media in Indiana and neighboring Kentucky on January 27, 2015. The notification letters were sent to the printer on January 26th, and given the volume, were mailed out over the week. We have received confirmation from the printer that all of the letters will be in the mail on or before Monday, February 2, 2015.

The Resort is offering credit monitoring to those who receive letters (i.e., the best plan available through Experian, which covers all three credit bureaus and includes $1 million dollars in identity theft protection insurance coverage) and also established an internal call center, which is operational 7 days a week, from 7 am through 11 pm.

I have enclosed a copy of the notification letter, credit monitoring instructions and identity theft fact sheet which was included with the letters, as well as a copy of the press release. These materials were also attached to Matt Van Hise's email to you.

Please do not hesitate to let us know if you have any questions or would like any additional information.

Thank you.

Very truly yours,

[redacted]

Enclosures

PARK LEGAL LLC

[redacted]

FRENCH LICK RESORT

FRENCH LICK & WEST BADEN · INDIANA

January 26, 2015

[Insert credit monitoring enrollment authorization code here]

Dear _____,

The purpose of this letter is to inform you about a payment card incident that was identified by French Lick Resort. On January 19, 2015, we learned that a hacker installed malware (a software credit card scraping device) on some of our card payment devices, which compromised the security of the credit card systems that we use for purchases at our Resort by guests, visitors, and our associates.

What happened?

This situation was initially brought to our attention on January 13, 2015, by a bank that noticed credit card compromises relating to 28 cardholders who had all used their credit cards at our Resort. The Resort promptly investigated this situation with assistance from a nationally recognized IT security and forensics firm, and learned through that investigation that our point-of-sale (POS) system, which is used to process credit cards across our Resort, had been compromised by a hacker. (POS systems are the most likely way that credit card data can be stolen by a hacker and they have been implicated in most of the other major credit card breaches of retailers that have been reported by the media.)

Through that investigation, we learned that the hacker installed malware on the POS system on April 22, 2014, and activated it on April 23, 2014 to steal credit card numbers. The malware was concealed from detection by the hacker and unfortunately was not identified during the Resort's routine malware and spyware reviews or by our continually running software. On January 19, 2015, we detected the malware through our detailed forensics review, and our IT security team and external experts were able to confirm that it was disabled on January 21, 2015.

Because we want to ensure that every potentially affected customer (including our guests, visitors and associates) receives notification about this situation, we are sending this letter to all 85,975 individuals whom we can identify as visiting the Resort during the period when the malware was installed and active.

What is the Resort doing about this?

Upon learning about the potential credit card data compromise, we took immediate steps to evaluate it, block any further data leakage, and re-secure our systems. We are continuing to coordinate with cybersecurity and forensic specialists to gain a better understanding about how this situation occurred, and to apply additional safeguards to help prevent any compromises of security from happening again. We are also coordinating with the card brands and law enforcement officials to identify the hacker and pursue criminal enforcement.

Although affected cardholders are not responsible for unauthorized charges on their credit or debit cards if promptly reported to their bank or credit card company, we nevertheless recognize that you may be concerned because your data has been subject to unauthorized access. We are therefore providing one year of free credit monitoring services through Experian®, which is one of the three national credit bureaus. The services that we are providing include real-time monitoring of your credit reports via all three national credit bureaus, prompt notification to you in the event that anyone tries to establish credit in your name, a 24-hour help desk from Experian, and $1 million dollars

in insurance coverage per card number should any identity theft situations be linked to this situation. We also recommend individuals contact their credit card companies and request new, replacement cards.

The enrollment instructions to sign up for the credit monitoring are included with this letter, and require use of the one-time activation code contained under the date on the first page of the letter.

We have also set up an internal toll-free number for you to call if you have any questions or if you would like to talk with the Resort about this situation, or if you would like assistance enrolling in the credit monitoring program. The number is 877-664-3577, and our team is available every day (including Saturday and Sunday), from 7:00 am until 11:00 pm, Eastern time.

What can you do to protect yourself?

In addition to signing up for credit monitoring, we recommend that you carefully review your credit card statements to look for any unauthorized charges. You should do the same with any bank statements, particularly if you use debit cards. If you notice any unauthorized charges, you should contact your credit card company or bank immediately to dispute the charges. Doing so will not only protect you against having to pay for any unauthorized charges on your statement, but also will help the law enforcement agencies working with us gather all available evidence of unauthorized card usage, so that we can optimize our efforts to identify and bring the hackers to justice.

Because identity theft is a widespread concern that can occur in many ways, we are also enclosing an Identity Theft Information Sheet. We recommend that you review and follow the recommendations in the Information Sheet and take advantage of the resources that are identified on it to obtain more information, such as those that are available through the Federal Trade Commission's consumer protection and identity theft division, as well as similar divisions that have been established by the attorney general's offices in each state. As explained more fully on the fact sheet, you also have the option to apply a "credit freeze" through the three national credit bureaus (Experian, Equifax, and TransUnion). A credit freeze puts a full block on access to your credit, so that no one can take out credit in your name without your permission.

Where can you go for more information or questions?

If you have concerns or questions, you can call our toll-free number (877-664-3577). You can also use the resources identified in the attached identity theft fact sheet.

****

We apologize for this situation and any inconvenience this may have caused. We want to thank you for your patronage and support as we work through this matter, and assure you that we have and are continuing to take swift and comprehensive steps to ensure a solid level of protection for all credit card and other personal data entrusted to us by our guests, visitors, and associates.

Very truly yours,

Chris B. Leininger
Chief Operations Officer

FRENCH LICK RESORT

FRENCH LICK & WEST BADEN · INDIANA

Instructions for Activating the Experian® ProtectMyID™ Now in Three Easy Steps

1. ENSURE **that you enroll by May 31, 2105.** (Your code will not work after this date.)
2. Visit the **ProtectMyID website to enroll: www.protectmyid.com/redeem**
3. PROVIDE **your activation code. Your activation code can be used by only you. It is included in the upper right-hand corner of your notification letter from French Lick Resort, just below the date of the letter.**

If you have questions or need an alternative to enrolling online, please call Experian's customer care team at **(866) 584-9681**. You will be asked to provide your engagement number, which is: **PC91655 (if you received a notification letter)**

Additional details regarding your 12-MONTH ProtectMyID membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance alerts for:**
  - **Daily bureau credit monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity theft resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated identity-theft resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts, including credit, debit and medical insurance cards; assist with freezing credit files; and contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high level of fraud resolution *support* even after your ProtectMyID membership has expired.

FRENCH LICK RESORT

FRENCH LICK & WEST BADEN · INDIANA

Identity Theft Protection Sheet
Tips to Protect Your Personal Information

Offline ■ Online ■ Mobile Devices ■ Family Members

Double-check credit card and other financial statements

As soon as your statement arrives, review it carefully to make sure it is accurate. If there are any discrepancies or signs of fraudulent activity, deal with them right away by calling the financial institution and disputing the charge. Keep a record of all disputes, and, if appropriate, contact your local police, the US Federal Trade Commission (www.consumer.FTC.gov), or your state attorney general's office (Consumer Fraud Unit) for assistance or additional information.

Protect and periodically evaluate your credit

Check your credit report regularly to make sure that no fraudulent credit cards are opened in your name. With a stolen Social Security number or driver's license number, someone can set up a new credit card account with a fake address and phone number. To get a free copy of your credit report, which reflects your credit at all three national credit bureaus, go to www.annualcreditreport.com or call 1-877-322-8228.

Consider applying a credit freeze

The best way to protect your credit is to apply a credit freeze. A credit freeze blocks anyone from accessing your credit report for purposes of establishing new credit in your name. Although there is a small charge for applying a freeze (up to $15 for each of the three national credit bureaus if you have not had your identity stolen, and another $15 if you want to lift the freeze to authorize new credit in your name), this is a small price to pay in comparison to the hassle and costs of addressing identity theft. To apply a freeze, contact *all three* national credit bureaus: Equifax at 1-800-525-6285, Experian at 1-888-397-3742, and TransUnion at 1-800-680-7289.

Keep your offline information secure

When disposing of sensitive materials, especially financial statements and pre–approved credit card offers, destroy them by putting them through a shredder. Opt-out of free credit card offers. Ensure that your financial information is securely stored at home and away from unauthorized people who could access it.

Protect your postal mail

Pick up your mail as soon as possible. A box stuffed full of catalogs, letters, and credit card statements can be awfully tempting to would-be thieves. If you won't be able to pick up your mail, have someone you trust do it. Or better yet, have the post office hold onto it for you. Also, bring any outgoing mail to the post office or to a drop box rather than leaving it in your mailbox.

FRENCH LICK RESORT

FRENCH LICK & WEST BADEN · INDIANA

Protect your Social Security number

When companies ask for your Social Security number (SSN), ask why they need it and how they will safeguard it. It's your SSN, after all. If you are uncomfortable giving it out, just say no. Also, try not to let companies use your SSN as an identification number, especially if it will appear multiple times. If your driver's license number is your SSN, ask to have it changed.

Be careful when sharing personal information

Don't give out personal information over the phone, by mail, or on the Internet unless you really know who you are dealing with. Never click on attachments or links in emails unless you know the sender. If the email message seems strange or out of character for the sender, don't click on the attachment, because the email sender could be a thief impersonating the individual that you know.

Be smart about using ATMs

Pay attention when using an ATM and be alert for anyone who seems a little too interested in your transactions. When possible, use your free hand to shield the keypad when entering your PIN. Also, try to avoid "sketchy" ATMs. Some ATMs have been set up to copy your account number while still giving you money. If you must use an ATM, use one that is located at a bank (rather than at a hotel, convenience store, mall, or other location).

Be smart about online banking

Although the banks have taken very strong measures to protect you, online banking still presents risks. Thieves can install malware on your computer or mobile device and then steal your banking credentials and make withdrawals from your account. Similarly, they can copy your credentials while you are engaging in online banking. Unlike the protections that are in place to protect you from fraudulent credit card charges, there are generally no protections against fraudulent withdrawals from your accounts. You will have to convince your bank or financial organization that the transaction was fraudulent, which, as you can imagine, can be quite challenging to do.

Use a strong password

While it is tempting to use the same short and simple combination for all your accounts, it makes it that much easier for someone to steal access to your accounts. You should use a strong password that contains a random combination of letters, numbers, and symbols for increased protection. Using your dog's name or 123456 is never a good idea. One easy way to create a challenging password is to think of a favorite phrase or song, and use the first letter of each word as your password, along with a few numbers or symbols.

Keep your credit cards to a minimum

The fewer credit cards you have, the better. Keep only the ones you actually use or plan to use. Also, keep organized records of all your credit cards and their billing cycles so you can report a theft promptly and thoroughly. And, carry with you only the cards that you need (in case your wallet or purse is lost or stolen). Safeguard the others in a secure location.

Secure your personal computing devices

Be sure that your personal computing devices have up-to-date antivirus software protections, malware protection, and—ideally—encryption. You can seek assistance from a computer or office supply store if you need help. This will help prevent hackers from gaining illicit access to your computer. Power off your devices when not in use or when you will be away from them for a period of time.

Don't overshare on social networking sites

Limit the personal information that you provide on social networking sites, especially if the site doesn't allow you to limit the information to friends only. Your and your children's dates of birth can be useful to identity thieves to help them re-create your identity. If you have a Facebook site, use the privacy settings to limit access to your information to the people that you choose to view it.

Be smart about smart phones and apps

Ensure that your personal devices, such as smart phones, are password protected, and, if they have such an option, turn on the remote wiping or "where's my phone" options so that you'll be able to remove your data if the device is lost, stolen, or corrupted. Be sure to back up your contacts and other information regularly. Install new operating systems and updates when prompted by the manufacturer. Evaluate your apps carefully before downloading them. Free apps are not always "free," because many have not been adequately tested and contain (or permit) malware.

Be wise about wi-fi

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

Read privacy policies

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information; and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

Protect your children's and elderly parents' identity

Identity theft is not limited to young adults. An increasing percentage of children and elderly adults have also been subject to identity theft. Be sure to safeguard your children's Social Security numbers and teach them not to disclose information that could be used by identity thieves. At the same time, remember that aging parents are often happy to receive telephone calls, including calls from strangers. They also may not be as technologically savvy as younger people about ensuring that their computers or smart phones have antivirus software on them. And, they may not recognize the importance of using strong passwords, or may write down their passwords on sticky notes and paste them to their computer or put them in a drawer. Make them aware of the current risks and show them what they need to do to best protect themselves.

FRENCH LICK RESORT

FRENCH LICK & WEST BADEN · INDIANA

Be aware of tax, medical, and other types of identity theft

Finally, you should be aware that identity theft isn't limited to opening new credit in your name. It also includes, for example, tax-related ID theft, medical or health insurance ID theft, and driver's license ID theft. You can get more information about the various types of identity theft and what you can do to protect yourself through the resources below.

Additional resources

www.consumer.ftc.gov; www.ftc.gov/idtheft

FRENCH LICK RESORT

FRENCH LICK & WEST BADEN · INDIANA

January 27, 2014

FOR IMMEDIATE RELEASE:

French Lick Resort confirms theft of guest credit cards

French Lick, Ind. – On January 13, the accounting department at the French Lick Resort learned of a possible compromise to its credit card payment system. After thorough review and internal investigation that involved the services of an expert IT data security company, it has been determined that credit and debit card numbers belonging to guests and visitors of the Resort may have been compromised. Any visitors to the resort between April 23, 2014 and January 21, 2015 who used a credit card may be affected by the theft.

The investigation revealed that malware was introduced to the payment system. That malware threat has been addressed. No credit cards used at the Resort after January 21 are believed to be at risk.

"Many members of the community, our employees, and friends of the resort could be among the guests whose credit card information was compromised," said Chris Leininger, chief operations officer of French Lick Resort. "We hope to contact anyone who could have been affected by this to ensure that they can act to protect themselves."

Anyone who used a credit or debit card at the resort between April 23, 2014, and January 21, 2015 could be at risk. If you have any questions about if you were affected or what you should do next, call the resort at 877-664-3577.

For anyone who was affected by this issue, we are offering a year of free identity protection.

"Identity theft can be unsettling and scary," said Chris Leininger. "We're truly sorry that our guests have to experience this, and we'll do our utmost to prevent anything like this from happening in the future."

- end text -

[redacted]