

2015116719



STATE OF NH  
DEPT OF JUSTICE  
2016 OCT 16 PM 12:09

office | 720.904.6010  
direct | 720.904.6021  
fax | 720.904.6020  
cmcnicholas@halewestfall.com  
1600 Stout Street, Suite 500  
Denver, Colorado 80202  
www.halewestfall.com

Christopher M. McNicholas | Attorney

October 13, 2015

**By Regular Mail**

Consumer Protection and Antitrust Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Data Security Event

To Whom It May Concern:

We represent Service Systems Associates, Inc. ("SSA"), 4699 Marion Street, Denver, Colorado 80216, and are writing to notify you of a data security incident that may have compromised the security of personal information of an unconfirmed number of New Hampshire residents.

Service Systems Associates provides visitor services to cultural attractions in cities throughout the United States. The affected individuals, which may include New Hampshire residents, were visitors to gift shops in 10 zoos, museums, and other attractions located in California, Florida, Hawaii, Michigan, Pennsylvania, and Texas. Service Systems Associates does not have access to contact information for any of the affected individuals and, as a result, has provided substitute notice and media notice to affected individuals on October 13, 2015, in substantially the same form as the notice attached as Exhibit A.

The investigation into this event was completed by Sikich, an independent forensic investigator, with the final report provided to SSA on September 25, 2015. To date, SSA has not received the final number of potentially affected consumers. By providing this notice, Service Systems Associates does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

***Nature of the Data Security Event***

On June 18, 2015, Service Systems Associates discovered suspicious activity on several of its point of sale systems and immediately began an investigation to identify and remediate any security vulnerability. Service Systems Associates also began working with law enforcement officials and a third party forensics team to investigate the incident. This notice has not been delayed because of any law enforcement investigation, but the Secret Service has been kept apprised of the breach and relevant information regarding the breach.

Service Systems Associates has determined that the security of some personal information contained on its systems has been affected. The personal information affected by this incident may include the following information relating to what SSA believes is approximately 60,000 individuals who used a credit or debit card at one of the limited number of gift shops in the aforementioned States between March 24, 2015 and May 20, 2015: cardholder name, expiration date, primary account number, and magnetic stripe data.

### ***Notice to Affected Residents***

Service Systems Associates immediately notified credit card companies of this incident, and those companies have assumed responsibility for notifying affected cardholders. Service Systems Associates does not have access to contact information for affected cardholders and, as a result, cannot provide individual notifications and cannot determine States of residence. Service Systems Associates has, however, provided substitute and media notice throughout the United States and has notified the relevant consumer reporting agencies. In addition, Service Systems Associates has provided on the front page of its website, [www.kmssa.com](http://www.kmssa.com), a link to details and updates regarding the incident and investigation. A copy of this website notice is attached as Exhibit B.

### ***Other Actions Taken***

Service Systems Associates takes this matter, and the security of the personal information in its care, seriously and has taken measures to restore the secure functionality of the affected systems. Upon discovering this data security compromise, Service Systems Associates took steps to identify and remediate potential vulnerabilities in its systems and enhance the security of its systems. Service Systems Associates continues to work closely with its third-party experts to fully remediate this incident. Remedial efforts include identifying and removing the malware that caused the breach, including dual authentication for remote access, encryption devices, and the elimination of keyboard based mag readers, among other things.

To support potentially affected individuals, Service Systems Associates has established a toll-free hotline to answer questions about this incident and to provide information relating to protection against identity theft and fraud. Service Systems Associates will provide affected individuals access to a one-year membership to credit monitoring and identity protection services through Experian, at no cost to the affected individual. Service Systems Associates has also worked closely with credit card companies and its payment processor, to ensure that affected individuals are notified of this incident.

Office of the Attorney General

October 13, 2015

Page 3

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security compromise, please contact me at (720) 904-6010.

Sincerely,



Christopher McNicholas

Enclosures

**NEWS RELEASE**

**Media Contacts:**

Kara Hamstra / Kyle Adams  
Sikich Marketing & Public Relations  
[khamstra@sikich.com](mailto:khamstra@sikich.com) / [kadams@sikich.com](mailto:kadams@sikich.com)  
312-541-9300 x 106 / 101

**Service Systems Associates, Inc. Victim of Data Security Breach**

**DENVER – Oct. 13, 2015** – Service Systems Associates, Inc. (SSA) was the victim of a payment security breach between March 24 and May 20, 2015. The breach occurred in the company's point-of-sale systems used by gift shops in several zoos.

The malware that caused the breach was identified and removed, and all visitors should feel confident using credit or debit cards anywhere in these facilities.

As soon as SSA learned about the attack, it investigated the breach, working alongside Sikich, an independent forensic investigator accredited by the Payment Card Industry Security Standards Council. At the same time, SSA also took several steps to improve its security and prevent future attacks:

The following locations were affected by the breach:

- Dallas Zoo
- Detroit Zoo
- El Paso Zoo
- Fresno Chaffee Zoo
- Herman Park Conservancy
- Honolulu Zoo
- Houston Zoo
- Zoo Miami
- Museum of Science and Industry (Tampa, Florida)
- Pittsburgh Zoo & PPG Aquarium

Sikich has confirmed that malware has been located and removed from all affected SSA clients. Neither the malware nor its known artifacts have been found at any other SSA client locations.

SSA collaborated with affected zoos to alert their patrons and notified the credit card companies of the situation. Guests who used retail facilities at the affected locations between March 24 and May 20, 2015, should visit SSA's [website](#) for more information. To help any guest affected by this data breach, SSA will offer one year of fraud protection. To learn more about how to enroll in this service, please also visit SSA's [website](#).

Consumers who see any fraudulent activity on a credit or debit card should contact the relevant card issuer as soon as possible. Most credit card companies do not hold customers liable for fraudulent charges if they are promptly reported.

Additionally, here is some advice from the Consumer Financial Protection Bureau:

*If you believe you are a victim of identity theft, you should contact one of the consumer reporting agencies listed below to place a fraud alert on your credit report. You only need to contact one of the three credit reporting companies to place an alert.*

- *TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790*
- *Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241*
- *Experian: 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9554, Allen, TX 75013*

*For more details on the steps to take if you are a victim of identity theft, visit the Federal Trade Commission's Identity Theft website at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.*

###

## Details on Service Systems Associates, Inc. Data Breach

We are providing this notification to report that Service Systems Associates, Inc. ("SSA") was recently the victim of a data security breach.

The incident occurred in the point-of-sale systems located in the gift shops of fewer than a dozen of our clients. This means that if a guest used a credit or debit card in the gift shop at one of the following partner facilities between March 24 and May 20, 2015, the information on that card may have been compromised: Dallas Zoo, Detroit Zoo, El Paso Zoo, Fresno Chaffee Zoo, Herman Park Conservancy, Honolulu Zoo, Houston Zoo, Zoo Miami, Tampa's Museum of Science and Industry, and the Pittsburgh Zoo & PPG Aquarium.

### *Investigation*

SSA takes this issue very seriously. As soon as we learned about the attack, SSA began working with law enforcement officials and a third-party forensic investigator, Sikich, to investigate the breach. Through this investigation, we learned that the security of some personal information, including names, and credit card numbers had been affected. SSA has also notified the major credit card companies of this situation and they are in the process of notifying their customers.

Though the investigation into this attack continues, this notice has not been delayed by law enforcement. SSA has taken steps to protect the personal information of guests from further unauthorized access, including identifying and removing the malware that caused the breach. SSA is also taking several steps to improve its security and prevent future attacks, including dual authentication for remote access, encryption devices, and the elimination of keyboard based mag readers, among other things.

### *Identity Protection Services*

Out of an abundance of caution, we are offering affected individuals access to one year of credit monitoring services at no cost. Information about these services may be obtained by e-mailing [servicesystems@protectmyid.com](mailto:servicesystems@protectmyid.com).

### *Protecting Yourself From Fraud*

We suggest that individuals who may have been affected by this incident remain vigilant by reviewing account statements for suspicious activity and monitoring free credit reports. Under U.S. law, individuals are entitled to a free annual credit report from each of the three major credit bureaus. To obtain a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, (877) 322-8228. Guests who view any fraudulent activity on a credit or debit card should contact the relevant card issuer as soon as possible. Most credit card companies do not hold customers liable for fraudulent charges if they are promptly reported.

If you believe you are a victim of identity theft, you should contact one of the consumer reporting agencies listed below to place a fraud alert or security freeze on your credit report. You only need to contact one of the three credit reporting companies to place an alert.

TransUnion:  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)  
Fraud Victim Assistance Division  
P.O. Box 6790  
Fullerton, CA 92834-6790

Equifax:  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374-0241

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

Suspected incidents of identity theft should be immediately reported to local law enforcement, the Federal Trade Commission, and your state Attorney General. State Attorneys General and the FTC may also have advice on preventing identity theft, including placing a fraud alert or security freeze on your credit files.

***For North Carolina and Maryland Residents***

We are required by Maryland and North Carolina state laws to notify you that you may obtain information about preventing identity theft by contacting the Maryland and North Carolina Attorneys 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](http://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](http://www.oag.state.md.us).

You may also contact the FTC at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261.

***For Residents of Massachusetts and West Virginia***

We are required by Massachusetts and West Virginia law to notify affected individuals (1) that they have the right to obtain any police report filed in regard to this incident; (2) that if they are the victim of identity theft, they also have the right to file a police report and obtain a copy of it; and (3) that they may place a security freeze on their credit reports.

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

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 in Massachusetts and \$5.30 in West Virginia to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

***Contact Information***

We will provide relevant updates on our website as soon as they may become available. SSA is available to answer any questions about the data security breach and the personal information maintained by SSA that may have been compromised, and to provide more information about the credit monitoring and identity protection services we are offering. We may be reached from 8:00 a.m. to 5:00 p.m. MST at ~~at [insert toll free information]~~, or ~~creditinvestigation@kmssa.com~~.

Again, we are very sorry for any inconvenience due to this situation.