



June 21, 2013

BY OVERNIGHT MAIL AND E-MAIL

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

Re: Vendini, Inc.; Update to Notification of Information Security Breach

Dear Sir or Madam:

This letter follows up on our letter dated June 4, 2013 (attached) regarding a recent security incident experienced at Vendini, Inc. As noted in that letter, Vendini is a service-provider and does not believe that it owns or licenses the personal information at issue. We therefore notified our business customers ("Members") during the week of May 21, but to date have not directly notified Members' consumers ("Patrons") residing in this state. We have been responding to requests and working with Members to assist with their Patron notification activities. We have also closely monitored the Patron notification process and the progress of our Members in this regard. Some Members have asked Vendini to help notify their Patrons. Others do not appear to have reached out to their Patrons yet.

To help our Members and their Patrons at this stage, Vendini will voluntarily undertake to notify Patrons who have not yet been notified by Members. We are informing our Members of this plan, and have asked that they let us know if they do not wish for Vendini to notify their Patrons (e.g., where a Member has already notified or plans to notify its Patrons). Our goal is to avoid situations in which a Patron receives multiple notices about the same incident. We expect to be in a position to begin sending notices to Patrons starting the middle of next week (week of June 24). We plan to email Patrons for whom we have email addresses; and we will send hardcopy letters to those Patrons for whom we have mailing addresses but no emails or whose emails are undeliverable. Note that we have already posted notice of the incident on our website and issued a press statement to national and state media outlets on May 24. Again, while Vendini does not believe that it has a statutory obligation to undertake this notification plan, we want to do this to help our Members and their Patrons. Fortunately, to date, we are not aware of any confirmed instances of identity theft or fraudulent transactions that were attributable to this incident.

Please feel free to contact me directly at 1-800-901-7173 (ext. 767).

Very truly yours,

*Keith Goldberg*  
Vice President, Marketing

VENDINI, INC.  
WWW.VENDINI.COM 1 (800) 901-7173

SAN FRANCISCO • BOSTON • CHICAGO • LOS ANGELES • NEW YORK



June 4, 2013

**BY OVERNIGHT MAIL**

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

Re: Notification of Information Security Breach

Dear Sir or Madam:

I write to inform you of a security breach incident at Vendini, Inc. Vendini is headquartered at 660 Market Street, San Francisco, CA 94104 and has regional offices in other locations in the United States. Vendini provides box-office and online ticketing services to entertainment venues (referred to as "members"), which include tour, casino, sports, and arts organizations in the U.S. and Canada. Vendini is a service provider to its member organizations, who in turn have consumers ("patrons") of their venues and events.

On April 25, 2013, Vendini detected an unauthorized intrusion into its web application server systems. It appears that the intrusion was criminally motivated and may have begun on or around March 29, 2013. Our internal investigation has determined that the intrusion affected electronically-stored personal data belonging to members' patrons. That data includes name, address, email, phone number, and credit card numbers and credit card expiration dates. Vendini does not store or maintain credit-card security access codes (e.g., CVV, CVV2, PINs), social security numbers, or consumer usernames or passwords.

Upon detecting the intrusion, Vendini took immediate steps to begin remediation efforts. We retained outside forensic and cyber-security experts and commenced an internal investigation. We restricted the access point used by the intruder, upgraded our web server network system and security patches, and have taken additional steps to further strengthen our security systems. We also alerted and have been cooperating with our merchant banks and the credit card companies. After consultation with federal law enforcement, who advised that broad disclosure of the incident could compromise law enforcement's investigation, Vendini delayed notification specifically to avoid such compromise to the investigation, which is ongoing.

As a service-provider, Vendini does not believe that it owns or licenses the personal information at issue, which Vendini maintains for purposes of providing contracted-for services for its member organizations. Accordingly, we have notified our members, but we have not at this time provided direct notice to all affected residents of this state. Rather, we have been responding to requests from members to assist them with their notification efforts. We will continue to monitor the foregoing processes and will update your office should anything change. We, of course, welcome the opportunity to discuss any questions you may have regarding this incident.

Please feel free to contact me directly at 1-800-901-7173 (ext. 767).

Very truly yours,

*Keith Goldberg*  
Vice President, Marketing

VENDINI, INC.  
WWW.VENDINI.COM 1 (800) 901-7173

SAN FRANCISCO • BOSTON • CHICAGO • LOS ANGELES • NEW YORK



**IMPORTANT INFORMATION. PLEASE READ IN ITS ENTIRETY.**

Dear Patron:

We regret to inform you that on April 25, 2013, Vendini, Inc. detected an unauthorized intrusion into its systems. Vendini provides box-office and online ticketing services to hundreds of entertainment venues, which include tour, casino, sports, and arts organizations across the U.S. and Canada. Based on Vendini's records, you used a credit card to make a purchase for an event that was processed through Vendini's service, and your information may have been involved in this incident.

If you have already received a letter from Vendini or a Vendini customer (an event venue or organization who uses our ticketing services), this letter concerns the SAME incident and we apologize for any inconvenience. We have been working with our customers for several weeks, and we decided at this point to reach out directly to give you more information about what happened.

We are actively cooperating with federal law enforcement, and this notification to you was delayed to avoid compromising law enforcement's investigation. In addition, we have been conducting a full-scale internal investigation at Vendini with outside computer forensic and cyber security experts. Although these investigations are ongoing, Vendini believes that in late March, a third-party criminal actor used hacking technologies to access its databases and may have accessed **your personal information, such as name, mailing address, email address, phone number, and credit card numbers and expiration dates.** Please note that security access codes – such as the three-digit code that appears on the back of some credit cards (e.g., CVV, CVV2) – and PIN numbers, usernames, passwords, and Social Security Numbers were not affected, as Vendini does not collect and store this type of information.

We have implemented enhanced security measures designed to prevent a recurrence of this type of incident. We have cooperated and will continue to cooperate with federal law enforcement, our merchant banks and the credit card companies. In addition, please note the following:

- To protect against even the possibility of identity theft or fraud, we urge you to remain vigilant, and to regularly review your credit card account statements and credit reports for any unauthorized activity.
- If you suspect that you may be a victim of identity theft or fraud, immediately contact your local law enforcement agency, your State Attorney General's office and the Federal Trade Commission. We have enclosed a *Resources Guide* for your reference.
- Do NOT respond to any requests for sensitive personal information in relation to this incident. Vendini will never request such information via email or telephone unless it is absolutely necessary to respond directly to you regarding how this incident may impact you.

We sincerely regret this incident. Protecting data privacy and security is a top priority for Vendini, Inc. For more information regarding this incident, please contact Vendini toll-free at 1-800-836-0473 or visit [www.vendini.com/info](http://www.vendini.com/info).

Sincerely,

*Mark Tacchi*  
President and CEO

## RESOURCES GUIDE

**For Residents of Maryland and North Carolina:** For information about fraud alerts, security freezes, and steps you can take to protect against identity theft or fraud, contact the U.S. Federal Trade Commission (see contact information below), or as applicable:

**Maryland's Office of the Attorney General:** 200 Saint Paul Place, Baltimore, MD 21202; Tel: (410) 576-6300; or Visit: [www.oag.state.md.us](http://www.oag.state.md.us)

**North Carolina's Attorney General's Office:** 9001 Mail Service Center, Raleigh, NC 27699-9001; Tel: (919) 716-6400; Fax: (919) 716-6750; or Visit: <http://www.ncdoj.com>

---

**For Residents of Nebraska:** The Nebraska Attorney General's Identity Theft Repair Kit is available online at [www.ago.ne.gov/consumer\\_protection](http://www.ago.ne.gov/consumer_protection). The Nebraska Attorney General's Consumer Protection Mediation Center, which provides assistance to Nebraskans with consumer protection and identity theft issues, may be reached at (800) 727-6432 or (402) 471-2682, or by visiting [www.ago.ne.gov](http://www.ago.ne.gov).

---

**U.S. Federal Trade Commission (FTC):** The FTC has helpful information about how to avoid identity theft and other steps that consumers can take to protect themselves.

Write to: Consumer Response Center, 600 Pennsylvania Ave., NW, H-130, Washington, D.C. 20580  
Call Toll-Free: 1-877-IDTHEFT (438-4338); or Visit: <http://www.ftc.gov/idtheft>

---

**Free Annual Credit Report:** You may obtain a free copy of your credit report once every 12 months (or purchase or obtain additional copies of your credit report). Call Toll-Free: 1-877-322-8228; or Visit: <https://www.annualcreditreport.com>; or Contact any one or more of the national consumer reporting agencies:

<b>Equifax:</b>	P.O. Box 740241, Atlanta, GA 30374-0241	(800) 685-1111	<a href="http://www.equifax.com">www.equifax.com</a>
<b>Experian:</b>	P.O. Box 2002, Allen, TX 75013	(888) 397-3742	<a href="http://www.experian.com">www.experian.com</a>
<b>TransUnion:</b>	P. O. Box 1000, Chester, PA 19022	(800) 888-4213	<a href="http://www.transunion.com">www.transunion.com</a>

---

### "Fraud Alerts" and "Security Freezes"

**Fraud Alert** - You have the right to place a fraud alert in your file to alert potential creditors that you may be a victim of identity theft. Creditors must then follow certain procedures to protect you; therefore, a fraud alert may delay your ability to obtain credit. An "initial fraud alert" stays in your file for at least 90 days. An "extended fraud alert" stays in your file for 7 years, and will require an *identity theft report* (usually, a filed police report). You may place a fraud alert by calling any one of the three national consumer reporting agencies:

**Equifax:** 1-800-525-6285      **Experian:** 1-888-397-3742      **TransUnion:** 1-800-680-7289

**Security Freeze** - Some U.S. states provide the right to place a security freeze on your credit file, which prevents credit, loans and services from being approved in your name without your consent. Using a freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. To place a freeze, you must send a written request to **each** of the three major consumer reporting agencies (**addresses below**) with the following (if you are requesting for your spouse, this information must be provided for him/her as well): (1) Full name, with middle initial and any suffixes; (2) Social Security Number; (3) Date of Birth; (4) Current address and any previous addresses for the past several years; and (5) Any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles or other complaint concerning identity theft; (6) A copy of a government-issued identification card and (7) A copy of a recent utility bill or bank or insurance statement for proof of current address. Copies of documents must be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies have three (3) business days after receiving your request to place a security and must send you 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. There are also procedures for lifting and removing a freeze. The credit reporting agency may charge a fee up to \$5.00 to place, lift, and/or remove a freeze, unless you are a victim of identity theft and you have submitted a valid police report to the credit reporting agency. Do not send cash through the mail.

**Equifax Security Freeze:** P.O. Box 105788, Atlanta, Georgia 30348 ([www.equifax.com](http://www.equifax.com))

**Experian Security Freeze:** P.O. Box 9554, Allen, TX 75013 ([www.experian.com](http://www.experian.com))

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