Demers, Janet

From: Malone, Amy [ALMalone@mintz.com]
Sent: Tuesday, July 02, 2013 4:23 PM
To: DOJ-CPB
Subject: Breach Notification
Attachments: Suffolk_NH Notification.pdf

Dear Attorney General Foster,

Attached please find notice of a security breach from Suffolk University.

If you have any questions please don't hesitate to contact me.

Sincerely,

Amy Malone

Amy Malone | Attorney
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
One Financial Center | Boston, MA 02111
Direct: (617) 348-3099 | Fax: (617) 542-2241
E-mail: ALMalone@mintz.com
Web: www.mintz.com

MINTZ LEVIN

Cynthia J. Larose | 617 348 1732 | cjlarose@mintz.com

One Financial Center
Boston, MA 02111
617-542-6000
617-542-2241 fax
www.mintz.com

July 2, 2013

Via Email Transmission and Overnight Delivery

The Honorable Joseph Foster
Attorney General for the State of New Hampshire
33 Capitol Street
Concord, NH 03301

Re: Reporting of Security Breach

Dear Attorney General Foster:

This law firm represents Suffolk University ("Suffolk") in connection with a security breach incident that we believe to have taken place in late March 2013. On May 21, 2013 Suffolk was notified by its vendor, Vendini, Inc., a provider of box office and online ticketing services, of an incident involving the personal information of Suffolk patrons ("Vendini Initial Notice"). In the notification Suffolk received on May 21st, Vendini indicated that their investigation was not complete and that Vendini would fully investigate the matter and keep Suffolk up to date on developments. On June 17, 2013 Vendini provided an update on the security breach incident ("Vendini Follow-up Notice"). Copies of both notices are attached for your information. According to the Vendini Initial Notice, Vendini first detected an unauthorized intrusion by hackers into their computer systems on April 25, 2013 and since that time there has been no further intrusion into their systems. Based on Vendini's investigation, and according to the Vendini Initial Notice, a number of Suffolk patrons who used credit cards to purchase tickets through the Vendini services may have been affected. Further details regarding the Vendini investigation and its explanation for delay in notice to customers such as Suffolk can be found in the Vendini Follow-Up Notice. Although Suffolk University provides a web link to the Vendini website on the University's website, ticket purchases occur solely through Vendini, and personally identifiable information that patrons provide is transmitted, stored and maintained by Vendini on Vendini servers, and not with Suffolk University.

According to the Vendini Follow-Up Notice, in response to this security breach and the investigation conducted by Vendini's forensic experts, Vendini has restricted access points in their system, implemented additional monitoring processes to allow for quicker detection of unauthorized activity in their database environment and increased security around information protection, including increasing the encryption used for credit card data. Suffolk has no actual knowledge of how or whether credit card numbers were encrypted in the Vendini database prior to the breach, but Suffolk's contractual agreement with Vendini does contain representations and warranties from Vendini that it would maintain compliance with PCI-DSS requirements.

While Suffolk has no knowledge of any patron information being used improperly, out of an abundance of caution, Suffolk is notifying your office and affected patrons

regarding this incident. Based on the review of Vendini's files provided to Suffolk, approximately 132 New Hampshire residents transacting via the Suffolk website may have been affected by this incident. Although we have received no reports of fraudulent charges from New Hampshire residents, the enclosed notice will be provided to alert them to be vigilant. As a precautionary measure, Suffolk is offering a credit monitoring and credit protection service provided by AllClear ID. Suffolk has also contracted with AllClear ID to provide a dedicated call center for affected patrons to call with questions regarding this incident.

The letter being sent to New Hampshire residents commencing this week is attached. Notice has also been posted to the Suffolk website at www.suffolk.edu.

If you have any questions or concerns, please do not hesitate to contact me at (617) 348-1732.

Sincerely,

Cynthia J. Larose

IMPORTANT INFORMATION.
PLEASE READ IN ITS ENTIRETY.

May 21, 2013

Dear Member:

We regret to inform you that on April 25, 2013, Vendini detected an unauthorized intrusion into its systems. This incident affected our members' patrons who have used a credit card to make a purchase for an event that was processed through Vendini services.

We are actively cooperating with federal law enforcement, and this notification to you was delayed to support law enforcement's investigation. In addition, a full-scale, internal investigation is under way at Vendini with computer forensic and cyber security experts. Although our internal investigation is ongoing, we believe that in late March, a third-party criminal actor used hacking technologies to access our databases and may have accessed personal information, such as name, mailing address, email address, phone number, and credit card numbers and expiration dates that belong to our members' patrons. We do *not* collect credit card security access codes (e.g., CVV, CVV2, PINs) or social security numbers, patron usernames or passwords.

Upon discovering this intrusion, we engaged computer forensic and cyber security experts to commence an investigation. We implemented enhanced security measures designed to prevent a recurrence of this type of incident. At this time, we do not believe that this incident affects sales after April 25, 2013.

In the next day or so, Vendini will as appropriate directly notify certain affected patrons to provide information resources and encourage them to take steps to protect themselves from potential unauthorized use of their credit card. We recommend that you consult with your counsel regarding legal duties you may have in connection with this incident, including any obligation you may have to notify your patrons separately of Vendini.

If you process credit cards through Vendini's merchant account, we have already notified our merchant banks; and credit card companies have also been alerted. If you process credit cards through your own merchant accounts, you may want to reach out to your merchant bank and notify them of this issue. If they have further questions they can contact Vendini toll-free at 1 (800) 901-7173.

We deeply regret this incident and are taking proactive steps to prevent it from happening again. We will continue to help federal law enforcement catch and prosecute the perpetrator. Our business is built on our ability to provide trusted

services to our members and their patrons. This trust is founded on data protection and privacy, which is our highest priority.

You have our assurance that we will work diligently to fully investigate this matter and keep you up to date on developments. We are fully committed to our members and will work diligently to maintain your trust and confidence.

Should you have any questions about this matter, please contact your member advocate, or call toll-free 1 (800) 901-7173.

Sincerely,

Mark Tacchi
President and CEO

Attachment: Patron Letter to be sent by Vendini:

==========

IMPORTANT INFORMATION. PLEASE READ IN ITS ENTIRETY.

May 22, 2013

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 our 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.

We are actively cooperating with federal law enforcement, and this notification to you was delayed specifically to support law enforcement's investigation. In addition, a full-scale, internal investigation is under way at Vendini with outside computer forensic and cyber security experts. Although our internal investigation is ongoing, we believe that in late March, a third-party criminal actor used hacking technologies to access our databases and may have accessed your personal information, such as name, mailing address, email address, phone number, and credit card numbers and expiration dates. We do not collect credit card security access codes (e.g., CVV, CVV2, PINs), social security numbers, usernames or passwords.

Upon discovering this intrusion, we engaged computer forensic and cyber security experts to commence an investigation. We implemented enhanced security measures designed to prevent a recurrence of this type of incident. We notified our merchant banks; and credit card companies have been alerted.

In addition, please note the following:

- To protect against 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 our company. For more information regarding this incident, please contact us toll-free at 1-800-836-0473 or visit us at 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, 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

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

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 of 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:
Equifax: P.O. Box 740241, Atlanta, GA 30374-0241 (800) 685-1111 www.equifax.com
Experian: P.O. Box 2002, Allen, TX 75013 (888) 397-3742 www.experian.com
TransUnion: P. O. Box 1000, Chester, PA 19022 (800) 888-4213 www.transunion.com

"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 interfere with or delay your ability to obtain credit. To place a freeze, send a request by mail to each consumer reporting agency (addresses below) with the following (if you are requesting a credit report 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 two years; and (5) Any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. You must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. Each copy must be legible, display your name and current mailing address, and the date of issue. 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 or the spouse of a victim of identity theft, and you have submitted a valid police

report relating to the identity theft incident to the consumer reporting agency.
Equifax Security Freeze: P.O. Box 105788, Atlanta, Georgia 30348
Experian Security Freeze: P.O. Box 9554, Allen, TX 75013
TransUnion (Fraud Victim Assistance Division): P.O. Box 6790, Fullerton, CA 92834-6790

Unsubscribe

View as a web page.

From: Vendini Support <support@vendini.com>
Date: Mon, 17 Jun 2013 13:50:24 -0700
To: Rachel Cardillo <rcardillo@suffolk.edu>
Subject: Vendini Update

Hi,

I want to give you an update on the data breach. We've had a lot of eyes on our systems over the past several weeks scrutinizing all the details. Since April 25, we have seen no evidence of further intrusion into Vendini's systems. We are also working closely with all patrons we've contacted and those who've contacted us to ensure their safety and security.

This was a sophisticated criminal attack and we have upgraded and further enhanced our security to prevent this type of intrusion from recurring. More specifically, we have restricted access points to our system, implemented additional monitoring processes to allow for quicker detection of unauthorized activity in our database environment and increased security around information protection, including increasing the encryption used for credit card data. We've done this work with the assistance of forensics and cyber-security experts.

We have seen the attackers contact Members via email, apparently offering to help, possibly in an attempt to obtain sensitive information from you. Please notify us immediately if you are unsure of any contact you receive about this matter other than from Vendini.

We've had questions about why we took so long to notify you and patrons about this breach. We consulted federal law enforcement immediately when we learned about the incident, and we delayed notifying solely to avoid compromising their investigation. The investigation is ongoing, we are cooperating and providing information, and we hope it will result in an apprehension of the attackers. We have worked closely with federal law enforcement to ensure we could notify as soon as possible without jeopardizing their investigation. They kept us up to date throughout their investigation. As soon as they felt it was appropriate and would not jeopardize their investigation, we notified you.

As part of the normal process, Visa and the other card brands appoint an independent forensics investigator and they should be wrapping up their findings shortly. We have also hired our own security forensics firm that has advised us on hardening the system. In addition, we have also been going through our regular annual renewal process for our PCI compliance and should have our new Report on Compliance shortly. We are working to ensure that our PCI compliance is maintained and uninterrupted.

I truly appreciate your commitment to Vendini as we build a stronger and more secure company. Thank you for being a customer.

Mark Tacchi
President & CEO

[SUFFOLK UNIVERSITY LETTERHEAD]

REDEMPTION CODE

Month ___, Year

Name
Address
City, State Zip

Dear _____,

This letter is to notify you of a recent incident that may have resulted in unauthorized access of some of your personal information.

Suffolk University contracts with a third-party vendor, Vendini, Inc. for box office and online ticketing services. Vendini recently informed the University that, on April 25, 2013, it detected an unauthorized intrusion into its systems that it believes to have taken place in late March 2013. Based on Vendini's records, you used a credit card to make a purchase for a Suffolk University event that was processed through Vendini's systems, and your information may have been involved in this incident. Vendini believes that the following personal information may have been accessed: name, mailing address, email address, telephone number and credit card numbers and expiration dates. Vendini does not collect credit card security access codes (e.g., CVV, CVV2, PINs,) or Social Security numbers, patron usernames or passwords.

Vendini reports that it is in contact with federal law enforcement and is cooperating with that ongoing investigation. In addition, Vendini also reports that, upon discovering the intrusion, it engaged computer forensic and cyber security experts to commence an investigation. It reports that it has implemented enhanced security measures designed to prevent a recurrence of this type of incident. To learn more about the breach, you may want to contact Vendini toll-free at 1-800-836-0473 or by visiting its website at www.vendini.com/info.

Suffolk University takes this matter seriously. To protect you from the possibility of unauthorized charges on your credit card, we recommend that you review all charges on your account for potentially fraudulent activity. Please note that you may have already received notice from Vendini, Inc. regarding this matter, and this letter relates to the same incident.

Please also review the detailed instructions that we have included with this letter relating to fraud alerts and security freezes and the information on receiving and reviewing your credit reports.

As an added precaution, Suffolk University has arranged to have AllClear ID provide you with fraud protection services for a year **at no cost to you.** The following identity protection services start on the date of this notice and you can use them at any time during the next year.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use this service – there is no action required on your part. If a problem arises, simply call <<Opportunity_Customer_Service_Number>> and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear ID has a 100% success rate in resolving financial identity theft issues and maintains an A+ rating at the Better Business Bureau.

AllClear PLUS: This service offers additional layers of protection including fraud detection that delivers secure, actionable alerts to you by phone and $1,000,000.00 Identity Theft Insurance Coverage. To use the PLUS service, you will need to provide your personal information to AllClear ID and use the following redemption code {RedemptionCode}. You may sign-up online at enroll.allclearid.com, by mail using the enclosed mail-in registration form, or by phone at <<Opportunity_Customer_Service_Number>>. Mailed registrations may take up to ten (10) business days before the registration is received and you are able to log-in to your account.

Suffolk University is committed to ensuring the privacy of all personal information and we expect all vendors with whom we do business to demonstrate the same level of commitment. We sincerely regret any inconvenience or concern that this matter may have caused you.

Yours truly,

Danielle Manning
Senior Vice President of Finance and Administration

RECOMMENDED STEPS TO HELP PROTECT YOUR IDENTITY

PLEASE NOTE: NO ONE IS ALLOWED TO PLACE A FRAUD ALERT ON YOUR CREDIT REPORT EXCEPT FOR YOU. PLEASE FOLLOW THE INSTRUCTIONS BELOW TO PLACE THE ALERT.

1. Request and Review Credit Reports

As a precautionary measure, **we recommend that you remain vigilant** by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained and request that the card or account be closed. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report is provided below:

Equifax	**Experian**	**TransUnion**
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate, and look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number provided on the report. When you review your credit card statements, look for charges you did not authorize and report these to your credit card issuer for investigation.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. Obtain a copy of the police report as you may need to give copies of the police report to creditors to clear up your records.

Even if you do not find signs of fraudulent activity on your reports, we recommend that you check your credit report every three months for the next year. To do so, just call one of the numbers above to order your reports and keep the fraud alert in place.

2. Place Fraud Alerts

Due to the nature of the information involved, you may wish to place a fraud alert with one of the three major credit bureaus. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change any of your existing accounts. A fraud alert can protect you but may also cause delays when you seek to obtain credit or activate credit monitoring. Contact information for the three bureaus and the website address for Experian are:

Equifax Fraud Reporting 800_ 525-6285 P.O Box 740241 Atlanta, GA 30374-0241	Experian Fraud Reporting 888- 397-3742 P.O Box 9532 Allen, TX 75013 www.experian.com	TransUnion Fraud Reporting 800- 680-7289 Fraud Victim Assistance Division P.O Box 6790 Fullerton, CA 92834-6790

You only have to contact ONE of the three bureaus to place a fraud alert. As soon as one of the three bureaus confirms your fraud alert, the others will automatically place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit or prevent the timely approval of any requests you make for new loans, 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 each 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 by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze Fraud Victim Assistance Department P.O. Box 6790 Fullerton, CA 92834

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 past five (5) 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 also must 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 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. This cannot be done by telephone. 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. They may charge you up to $5 each for such requests.

To remove the security freeze, you must send a written report to **each** of the three credit bureaus by mail and include proper identification (name, address, Social Security number) and the PIN 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. They may charge you up to $5 each for such requests.

4. Additional Information

You can obtain additional information about the steps you can take to avoid identity theft from the following:

For Maryland Residents
Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Telephone: 1-888-743-0023

For North Carolina Residents
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com
Telephone: 1-919-716-6400

For all other US Residents
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
(877)- IDTHEFT (438-4338)
TDD: 1-202-326-2502