Michaels
Where Creativity Happens

MICHAEL J. VEITENHEIMER
SVP, General Counsel & Secretary

T 972-409-1655
F 972-409-1965
veitenhm@michaels.com

April 18, 2014

New Hampshire Attorney General
Michael A. Delaney
33 Capitol Street
Concord, NH 03301

Dear Mr. Delaney:

I am writing to provide you with an update regarding the nature and circumstances of a data security issue previously reported to your office in a letter dated January 27, 2014.

On January 25, 2014, Michaels Stores, Inc. ("Michaels") informed its customers that the company might have experienced a data security issue. At that time, Michaels learned of possible fraudulent activity on some U.S. payment cards that had been used at Michaels stores. Since the announcement, Michaels retained two independent, expert security firms to conduct an extensive investigation. The company also has been working closely with law enforcement authorities and coordinating with banks and payment processors to determine the facts.

After weeks of analysis, Michaels discovered evidence confirming that systems of Michaels stores in the United States and its subsidiary, Aaron Brothers, were attacked by criminals using highly sophisticated malware that had not been encountered previously by either of the security firms. The affected U.S. systems contained certain payment card information, such as payment card number and expiration date, about both Michaels and Aaron Brothers customers. There is no evidence that other personal information of these customers, such as name, address or PIN, was at risk in connection with this issue.

Michaels has now identified and fully contained the incident, and the malware no longer presents a threat while shopping at Michaels or Aaron Brothers. Attached for your reference is a copy of the updated information Michaels posted on its website on April 17, 2014, describing the additional facts the company has determined from its continuing investigation. While Michaels has received limited reports of fraud, the company is offering identity protection, credit monitoring and fraud assistance services to affected Michaels and Aaron Brothers customers in the U.S. for 12 months at no cost to them.

Michaels is not able to determine the number of New Hampshire residents who might have been impacted by this issue.

If you have any questions, please do not hesitate to call me at 972-409-1655.

Very truly yours,

Michael J. Veitenheimer
SVP, General Counsel and Secretary

Enclosures

8000 Bent Branch Drive
Irving, TX 75063
972 409.1300

Michaels

April 17, 2014

Dear Valued Customers:

In January, we notified you that we might have experienced a data security incident. We wanted you to know quickly so you could take steps to monitor activity on your payment card account.

Since that time, we have continued our extensive investigation with the help of two independent, expert security firms. We have also been working closely with law enforcement authorities and coordinating with banks and payment processors to determine the facts.

After weeks of analysis, we have discovered evidence confirming that systems of Michaels stores in the United States and our subsidiary, Aaron Brothers, were attacked by criminals using highly sophisticated malware that had not been encountered previously by either of the security firms.

We want you to know we have identified and fully contained the incident, and we can assure you the malware no longer presents a threat to customers while shopping at Michaels or Aaron Brothers.

Here are additional facts we have determined from our continuing investigation:

- The affected systems contained certain payment card information, such as payment card number and expiration date, about both Michaels and Aaron Brothers customers. There is no evidence that other customer personal information, such as name, address or PIN, was at risk in connection with this issue.

- Regarding Michaels stores, the attack targeted a limited portion of the point-of-sale systems at a varying number of stores between May 8, 2013 and January 27, 2014. Only a small percentage of payment cards used in the affected stores during the times of exposure were impacted by this issue. The analysis conducted by the security firms and the Company shows that approximately 2.6 million cards may have been impacted, which represents about 7% of payment cards used at Michaels stores in the U.S. during the relevant time period. The locations and potential dates of exposure for each affected Michaels store are listed on www.michaels.com.

- Regarding Aaron Brothers, the Company has confirmed that between June 26, 2013 and February 27, 2014, 54 Aaron Brothers stores were affected by this malware. The Company estimates that approximately 400,000 cards were potentially impacted during this period. The locations for each affected Aaron Brothers store are listed on www.aaronbrothers.com.

- The Company has received a limited number of reports from the payment card brands and banks of fraudulent use of payment cards potentially connected to Michaels or Aaron Brothers.

We are truly sorry and deeply regret any inconvenience this may cause. Our customers are always our number one priority and we are committed to retaining your trust and loyalty.

While we have received limited reports of fraud, we are offering identity protection and credit monitoring services to affected Michaels and Aaron Brothers customers in the U.S. for 12 months at no cost to them. We also are offering these customers a fraud assistance service for 12 months at no cost to them. This service provides customers with a trained representative to assist them in the event they experience a fraud-related issue resulting from this incident. Information on the services can be found here.

We encourage you to actively monitor all of your payment card account activity and immediately contact your bank or card issuer if you notice any suspicious activity. You can find more security tips and information on this website.

In an era where very sophisticated and determined criminals have proven capable of successfully attacking a wide range of computer networks, we must all increase our level of vigilance. We are committed to working with other parties to improve the security of payment card transactions for all consumers.

If you have any questions or would like more information, please call us toll-free at 1-877-412-7145. Representatives are available to answer your questions Monday through Saturday from 8:00 a.m. CT to 8:00 p.m. CT.

We appreciate your patience and sincerely apologize again for any inconvenience this may have caused you. Thank you for your continued support.

Sincerely,

Chuck Rubin
CEO, Michaels Stores, Inc.

ADDITIONAL INFORMATION

Updated: April 17, 2014

We encourage our customers to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

We recommend that you remain vigilant by reviewing your credit reports. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Reporting Incidents. We encourage you to monitor your payment card account activity and immediately contact your bank or card issuer if you notice any suspicious activity. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement or your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW

Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Identity Protection and Credit Monitoring Services. While we have received limited reports of fraud, we are offering affected Michaels and Aaron Brothers customers in the U.S. identity protection, credit monitoring and fraud assistance services from AllClear ID for 12 months at no cost to them. These services start on April 17, 2014 and will be available at any time during the next 12 months.

AllClear SECURE: This service provides customers with a trained representative to assist them in the event they experience a fraud-related issue resulting from this incident. Affected Michaels and Aaron Brothers customers are automatically eligible to use this service – there is no action required on their part to enroll. Affected customers may receive this fraud assistance service by calling 1-877-412-7145.

AllClear PRO: This service offers credit monitoring and a $1 million identity theft insurance policy. Beginning on April 17, 2014, please click here to learn more and sign up for these services.

A customer is eligible for the services listed above if the customer used a payment card at:

- Any of the impacted Michaels stores in the U.S. during the affected time periods (by store); or
- Any of the 54 impacted Aaron Brothers stores between June 26, 2013 and February 27, 2014.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000	1-800-680-7289	www.transunion.com

	Chester, PA 19022-2000		

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the credit bureaus without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. For more information on security freezes, you may contact the three nationwide credit bureaus or the FTC as described above. Since the instructions for establishing a security freeze differ from state to state, please contact the three nationwide credit bureaus to find out more information.

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Proof of your current residential address (such as a current utility bill)
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. The credit bureaus may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit bureaus with a valid police report. You have the right to obtain a police report.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

FOR IMMEDIATE RELEASE

Media Contact:
Kim Paone
ICR, Inc. for Michaels
Phone: (646) 277-1216
Email: Kim.Paone@icrinc.com

Michaels Identifies and Contains Previously Announced Data Security Issue

IRVING, TX – April 17, 2014 – Michaels Stores, Inc. (the "Company" or "Michaels") today provided an update on its ongoing investigation into the data security issue it previously reported. In January, the Company learned of possible fraudulent activity on some U.S. payment cards that had been used at Michaels stores. Since the announcement, the Company retained two independent, expert security firms to conduct an extensive investigation. The Company also has been working closely with law enforcement authorities and coordinating with banks and payment processors to determine the facts.

After weeks of analysis, the Company discovered evidence confirming that systems of Michaels stores in the United States and its subsidiary, Aaron Brothers, were attacked by criminals using highly sophisticated malware that had not been encountered previously by either of the security firms.

The Company has now identified and fully contained the incident, and the malware no longer presents a threat while shopping at Michaels or Aaron Brothers. During the course of the investigation, the Company has determined the following:

- The affected systems contained certain payment card information, such as payment card number and expiration date, about both Michaels and Aaron Brothers customers. There is no evidence that other customer personal information, such as name, address or PIN, was at risk in connection with this issue.

- Regarding Michaels stores, the attack targeted a limited portion of the point-of-sale systems at a varying number of stores between May 8, 2013 and January 27, 2014. Only a small percentage of payment cards used in the affected stores during the times of exposure were impacted by this issue. The analysis conducted by the security firms and the Company shows that approximately 2.6 million cards may have been impacted, which represents about 7% of payment cards used at Michaels stores in the U.S. during the relevant time period. The locations and potential dates of exposure for each affected Michaels store are listed on www.michaels.com.

- Regarding Aaron Brothers, the Company has confirmed that between June 26, 2013 and February 27, 2014, 54 Aaron Brothers stores were affected by this malware. The Company estimates that approximately 400,000 cards were potentially impacted during

this period. The locations for each affected Aaron Brothers store are listed on www.aaronbrothers.com.

- The Company has received a limited number of reports from the payment card brands and banks of fraudulent use of payment cards potentially connected to Michaels or Aaron Brothers.

"Our customers are always our number one priority and we are truly sorry for any inconvenience or concern Michaels may have caused. We are committed to assisting affected customers by providing fraud assistance, identity protection and credit monitoring services. Importantly, with this incident now fully contained, we can assure customers this malware no longer presents a threat to shoppers at Michaels or Aaron Brothers," said Chuck Rubin, CEO.

Mr. Rubin added, "In an era where very sophisticated and determined criminals have proven capable of successfully attacking a wide range of computer networks, we must all increase our level of vigilance. Michaels is committed to working with all appropriate parties to improve the security of payment card transactions for all consumers."

The Company has provided data about potentially affected payment cards to the relevant card brands so they can take appropriate action. While the Company has received limited reports of fraud, it is offering identity protection, credit monitoring and fraud assistance services to affected Michaels and Aaron Brothers customers in the U.S. for 12 months at no cost to them. Details of the services and additional information related to the ongoing investigation are available on the Michaels and Aaron Brothers websites at www.michaels.com and www.aaronbrothers.com.

About Michaels and Aaron Brothers
Irving, Texas-based Michaels Stores, Inc. is North America's largest specialty retailer of arts, crafts, framing, floral, wall decor and seasonal merchandise for the hobbyist and do-it-yourself home decorator. Aaron Brothers, Inc. is a wholly-owned subsidiary of Michaels Stores, Inc. The Company currently owns and operates more than 1,135 Michaels stores in 49 states and Canada, and 119 Aaron Brothers stores in 9 states.

Updated: April 17, 2014

Website Frequently Asked Questions

1. What happened?

We previously informed our customers that we might have experienced a data security issue. Since the announcement, we retained two independent, expert security firms to conduct an extensive investigation. After weeks of analysis, we discovered evidence confirming that systems of Michaels stores in the United States and our subsidiary, Aaron Brothers, were attacked by criminals using highly sophisticated malware that had not been encountered previously by either of the security firms. The affected U.S. systems contained certain payment card information, such as payment card number and expiration date, about both Michaels and Aaron Brothers customers. We have now identified and fully contained the incident, and the malware no longer presents a threat while shopping at Michaels or Aaron Brothers.

2. Why is Michaels notifying Aaron Brothers customers?

Aaron Brothers is a wholly-owned and operated subsidiary of Michaels Stores, Inc. Our extensive investigation uncovered evidence confirming that systems of 54 Aaron Brothers stores were attacked by criminals using highly sophisticated malware. The affected systems contained certain payment card information, such as payment card number and expiration date, about Aaron Brothers customers who used payment cards at Aaron Brothers from June 26, 2013 to February 27, 2014.

3. What did Michaels do when it discovered the issue?

We previously informed our customers and relevant regulators that we might have experienced a data security issue. Since the announcement, we retained two independent, expert security firms to conduct an extensive investigation. We also have been working closely with law enforcement authorities and coordinating with banks and payment processors to determine the facts. As soon as available, we provided data about potentially affected payment cards to the relevant card brands so they could take appropriate action.

4. What information may have been compromised?

The affected U.S. systems contained certain payment card information, such as payment card number and expiration date, about both Michaels and Aaron Brothers customers. There is no evidence that other personal information of these customers, such as name, address or PIN, was at risk in connection with this issue.

5. Which Michaels stores in the U.S. were impacted by this incident?

The attack targeted a limited portion of the point-of-sale systems at a varying number of Michaels stores between May 8, 2013 and January 27, 2014. Only a small percentage of payment cards used in the affected stores during the times of exposure were impacted by this

issue. The analysis conducted by the security firms and Michaels shows that approximately 2.6 million cards may have been impacted, which represents about 7% of payment cards used at Michaels stores in the U.S. during the relevant time period. The locations and potential dates of exposure for each affected Michaels store are listed here.

6. Which Aaron Brothers stores were impacted by this incident?

We have confirmed that between June 26, 2013 and February 27, 2014, 54 Aaron Brothers stores were affected by this malware. We estimate that approximately 400,000 cards were potentially impacted during this period. The locations for each affected Aaron Brothers store are listed here.

7. Is it safe to use a payment card at Michaels and Aaron Brothers?

Yes. We have now identified and fully contained the incident, and the malware no longer presents a threat while shopping at Michaels or Aaron Brothers.

8. What should I do to help protect my information?

If you believe your payment card may have been affected, you should immediately contact your bank or card issuer. Under U.S. law, you are entitled to one free credit report annually from each of the three national credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. We encourage you to review your account statements and monitor your free credit reports. For more information about steps you can take to protect your credit files, you can contact any one of the consumer reporting agencies at:

Equifax	1-800-525-6285	www.equifax.com
Experian	1-888-397-3742	www.experian.com
TransUnion	1-800-680-7289	www.transunion.com

In addition, while we have received limited reports of fraud, we are offering identity protection and credit monitoring services to affected Michaels and Aaron Brothers customers in the U.S. for 12 months at no cost to them. We also are offering these customers a fraud assistance service for 12 months at no cost to them. This service provides customers with a trained representative to assist them in the event they experience a fraud-related issue resulting from this incident.

9. How do I find out more about the identity protection, credit monitoring and fraud assistance services?

We are offering affected Michaels and Aaron Brothers customers in the U.S. identity protection, credit monitoring and fraud assistance services for 12 months at no cost to them. Details of the services are available here. If you have any questions or would like more information, please call us toll-free at 1-877-412-7145, Monday through Saturday, from 8:00 a.m. CT to 8:00 p.m. CT.

10. Would Michaels ever contact me asking for my personal information?

No. Michaels will never ask you to provide personal information in an email or by telephone. You should always be suspicious of any unsolicited communication in which you are asked for your personal information or which refers you to a web page asking for personal information.

11. Where can I get more information?

If you have any questions or would like additional information regarding this issue, please call us toll-free at 1-877-412-7145, Monday through Saturday, from 8:00 a.m. CT to 8:00 p.m. CT.