WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

September 24, 2014

Melissa K. Ventrone
312.821.6105 (direct)
312.485.0540 (mobile)
Melissa.Ventrone@wilsonelser.com

Attorney General Tom Miller
Office of the Attorney General
Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

Dear Attorney General Miller:

We represent Jimmy John's Franchises LLC and are writing you on behalf of Jimmy John's Franchises LLC and its franchisees (collectively, "Jimmy John's") with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below. This letters serves as an update to our prior telephonic notification of September 02, 2014.

1. Nature of security incident.

On July 30, 2014, Jimmy John's learned of a potential security incident involving credit and debit credit card data at Jimmy John's stores and franchised locations. Jimmy John's immediately hired third party forensic experts to assist with its investigation. It appears that customer's credit and debit card data may have been compromised after an intruder stole log-in credentials from Jimmy John's point-of-sale vendor, Signature Systems, Inc. The intruder used these stolen credentials to remotely access the point-of-sale systems at some of Jimmy John's stores and franchised locations between June 16, 2014 and September 5, 2014. The security compromise has been contained, and Jimmy John's is processing credit and debit card data securely.

Approximately 216 stores appear to have been affected by this event. Cards impacted by this event appear to be those swiped at the stores, and did not include those cards entered manually or online. The credit and debit card information at issue may include the card number and in some cases the cardholder's name, verification code, and/or the card's expiration date. Information entered online, such as customer address, e-mail, and password, remains secure.

2. **Number of Iowa residents affected.**

At this time we cannot determine how many residents of Iowa may have been impacted by this event. However, there were four Jimmy John's locations within Iowa at issue. Attached for your reference is a

copy of the Substitute Notice posted on Jimmy John's web site at www.jimmyjohns.com.

3. **Steps you have taken or plan to take relating to the incident.**

Jimmy John's has taken steps to prevent this type of event from occurring in the future, including installing encrypted swipe machines, implementing system enhancements, and reviewing its policies and procedures for third party vendors.

Although the only information affected by this event was payment card information, Jimmy John's contracted with identity theft protection experts AllClear ID to provide identity theft restoration to impacted individuals at no cost to individuals for one year. Notice is also being provided to the credit reporting agencies.

4. Contact information.

Jimmy John's remains dedicated to the protection of the information in its systems. If you have any additional questions, please contact me at Melissa.Ventrone@wilsonelser.com, or (312) 821-6105.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Melissa K. Ventrone

Enclosure

cc: Kevin M Scott

FOR IMMEDIATE RELEASE

JIMMY JOHN'S NOTIFIES CUSTOMERS OF PAYMENT CARD SECURITY INCIDENT

CHAMPAIGN, Ill. (September 24, 2014) – On July 30, 2014, Jimmy John's learned of a possible security incident involving credit and debit card data at some of Jimmy John's stores and franchised locations. Jimmy John's immediately hired third party forensic experts to assist with its investigation. While the investigation is ongoing, it appears that customers' credit and debit card data was compromised after an intruder stole log-in credentials from Jimmy John's point-of-sale vendor and used these stolen credentials to remotely access the point-of-sale systems at some corporate and franchised locations between June 16, 2014 and September 5, 2014. The security compromise has been contained, and customers can use their credit and debit cards securely at Jimmy John's stores.

Approximately 216 stores appear to have been affected by this event. Cards impacted by this event appear to be those swiped at the stores, and did not include those cards entered manually or online. The credit and debit card information at issue may include the card number and in some cases the cardholder's name, verification code, and/or the card's expiration date. Information entered online, such as customer address, e-mail, and password, remains secure. The locations and dates of exposure for each affected Jimmy John's location are listed on www.jimmyjohns.com.

Jimmy John's has taken steps to prevent this type of event from occurring in the future, including installing encrypted swipe machines, implementing system enhancements, and reviewing its policies and procedures for its third party vendors.

We apologize for any inconvenience this incident may have on our customers. Jimmy John's values the privacy and security of its customers' information, and is offering identity protection services to impacted customers, although Jimmy John's does not collect its customers' Social Security numbers. To take advantage of these services, or for more information, call (855) 398-6442. In addition, customers are encouraged to monitor their credit and debit card accounts, and notify their bank if they notice any suspicious activity. Additional recommendations for protecting your information can be found at www.jimmyjohns.com.

Jimmy John's will post information related to its ongoing investigation on the Company's website, www.jimmyjohns.com.

FREE IDENTITY PROTECTION INFORMATION

Jimmy John's is taking every step to ensure your safety. The team at AllClear ID is ready and standing by if you need identity repair assistance. Access to this service is automatically available to you with no enrollment required for the next 12 months starting September 24, 2014. There is no action required on your part. If a problem arises, simply call 855-398-6442 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.

You are eligible to receive these services if you used a credit/debit card at one of Jimmy John's locations during the specific dates listed.

For additional details or questions regarding this incident, please visit www.JimmyJohns.com

Important Reminders:

- Your identity protection is completely free. You will never be charged.
- Review your credit card statements carefully and call your bank if you see any suspicious transactions.
- Be aware of phone calls or emails that appear to offer you identity theft protection but are truly phishing schemes designed to steal your information. Always go directly to our website or to the AllClear ID website for information rather than clicking on links in emails.

Recommendations to Our Customers

The security of our customer's information is our highest priority. Please review the following to learn about steps you can take to protect your information:

1. Monitor Your Payment Card Statements

We encourage our customers to always remain vigilant and monitor your accounts for suspicious or unusual activity. If customers observe unusual activity on an account, we advise that they contact their banks and/or credit card companies.

2. Monitor Your Credit Reports

We encourage our customers to monitor their credit reports. To order a free credit report, please visit www.annualcreditreport.com. Call 1-877-322-8228. Or complete an Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The FTC advises that you do not contact the three nationwide credit reporting companies individually, because they are providing free annual credit reports only through www.annualcreditreport.com, 1-877-322-8228 or mailing to Annual Credit Report Request Service.

Upon receipt of your credit report, we recommend that you review the "inquiries," section for names of any creditors from whom you have not requested credit, and the "personal information," section for any inaccuracies. Any unusual activity or information could be a sign of potential identify theft. If you observe such information, contact the credit bureau listed at the top of the report. Your credit report will be reviewed by the bureau staff with you, and if any information cannot be explained, you may need to contact the creditors involved.

3. Fraud Alerts

You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2020	P.O. Box 2000
Atlanta, Georgia 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com
1.800.525.6285	1.888.397.3742	1.800.680.7289

4. Security Freeze

You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security

freeze (note that 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 five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze and free if 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. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, Georgia 30348	Allen, TX 75013	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission. Please seethe FTC website at: www.ftc.gov.

5. Reporting Incidents

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*:
It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, Georgia 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of *Maryland, Illinois,* and *North Carolina*:
You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft/

For residents of *Massachusetts*:
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.