Representing Management Exclusively in Workplace Law and Related Litigation

jackson lewis.

Jackson Lewis P.C.
220 Headquarters Plaza
East Tower, 7th Floor
Morristown, NJ 07960-6834
Tel 973 538-6890
Fax 973 540-9015
www.jacksonlewis.com
Richard J. Cino - Managing Principal

ALBANY, NY	GREENVILLE, SC	MONMOUTH COUNTY, NJ	RALEIGH, NC
ALBUQUERQUE, NM	HARTFORD, CT	MORRISTOWN, NJ	RAPID CITY, SD
ATLANTA, GA	HONOLULU, HI*	NEW ORLEANS, LA	RICHMOND, VA
AUSTIN, TX	HOUSTON, TX	NEW YORK, NY	SACRAMENTO, CA
BALTIMORE, MD	INDIANAPOLIS, IN	NORFOLK, VA	SALT LAKE CITY, UT
BIRMINGHAM, AL	JACKSONVILLE, FL	OMAHA, NE	SAN DIEGO, CA
BOSTON, MA	KANSAS CITY REGION	ORANGE COUNTY, CA	SAN FRANCISCO, CA
CHICAGO, IL	LAS VEGAS, NV	ORLANDO, FL	SAN JUAN, PR
CINCINNATI, OH	LONG ISLAND, NY	PHILADELPHIA, PA	SEATTLE, WA
CLEVELAND, OH	LOS ANGELES, CA	PHOENIX, AZ	ST. LOUIS, MO
DALLAS, TX	MADISON, WI	PITTSBURGH, PA	TAMPA, FL
DAYTON, OH	MEMPHIS, TN	PORTLAND, OR	WASHINGTON, DC REGION
DENVER, CO	MIAMI, FL	PORTSMOUTH, NH	WHITE PLAINS, NY
DETROIT, MI	MILWAUKEE, WI	PROVIDENCE, RI	
GRAND RAPIDS, MI	MINNEAPOLIS, MN		

*through an affiliation with Jackson Lewis P.C., a Law Corporation

July 24, 2017

VIA ELECTRONIC MAIL
Direct of Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
Email: consumer@iowa.gov

Re: **Data Incident Notification**[1]

Dear Sir/Madam:

On July 4, 2017, our client, Avanti Markets Inc. ("Avanti Markets") was alerted to a sophisticated malware attack which affected kiosks it supports and that are maintained by its third party operators. The attack occurred as the result of an electronic intrusion at one of Avanti Markets' third party vendors. We are writing to inform you about the status of our investigation and Avanti Markets' significant remediation efforts.

Immediately upon learning of the incident, Avanti Markets commenced an investigation, including engaging a nationally-recognized forensic investigation team to help secure Avanti Markets' systems, confirm root cause, identify potentially affected individuals, and determine scope. The company also has been in communication with the Federal Bureau of Investigation and the United States Secret Service. This process is ongoing.

At this point, it appears the malware was intended to gather certain payment card information including the cardholder's first and last name, credit/debit card number, and expiration date. While improper access or acquisition of these data elements alone may not constitute a breach under the notification laws in all states, Avanti Markets is nevertheless alerting applicable state agencies of this incident. However, we have not been able to determine the number of affected individuals. As the investigation proceeds, Avanti Markets hopes to be able to provide more information.

Avanti Markets has taken numerous steps to secure its systems and the kiosks that are owned and operated by its operators and their customers. Prior to the incident, for example, many kiosks provided end-to-end encryption of payment card data and the company was implementing a plan to push that solution to all kiosks. Within hours of learning of the incident Avanti Markets took efforts to disable/remove the malware, shut down payment processing at some locations, advised operators to disconnect the card readers on the kiosks, and provided a notice for operators to display on the kiosks indicating that the card readers were unavailable. The company has been working with

[1] Please note that by providing this letter Avanti Markets is not agreeing to the jurisdiction of this state, or waiving its right to challenge jurisdiction in any subsequent actions.

jackson|lewis.

its operators to purge impacted systems of any malware from the attack with the goal of substantially minimizing the risk of data compromise. The company also deployed a sophisticated endpoint monitoring system to identify malware based on available definitions and prevent it from functioning.

At the same time, Avanti Markets commenced a communication strategy to ensure its operators and potentially affected customers received information about the incident. Within 3 days of discovering the incident, Avanti Markets provided initial notice to affected individuals via its website, along with a comprehensive set of Frequently Asked Questions. Additionally, Avanti Markets provided additional notice via state-wide media through the United States in an effort to reach affected individuals. Copies of the website notice, FAQs, and the state-wide media notice are attached. In the abundance of caution, Avanti Markets also has made credit monitoring services available to affected consumers at no cost.

As mentioned above, and as set forth in the attached notices, Avanti Markets treats all personal information in a confidential manner and is proactive in the careful handling of such information. Avanti Markets continues to assess and modify its privacy and data security policies and procedures to prevent similar situations from occurring. To this end, the company significantly advanced the implementation schedule of its end-to-end encryption solution for the kiosks, which as of this writing is 97% complete. Should Avanti Markets become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call us.

Sincerely,

JACKSON LEWIS P.C.

Joseph J. Lazzarotti
Jason C. Gavejian

Enclosure

4844-2704-7244, v. 1

CISION
PR Newswire

Avanti Markets Data Incident Notification

NEWS PROVIDED BY
Avanti Markets →
08:00 ET

TUKWILA, Wash., July 18, 2017 /PRNewswire/ --

To our Avanti Markets Community:

As most of you are aware by now, Avanti Markets suffered a data breach through a third party software provider over the July 4th holiday that impacted some Avanti Market kiosks.

Our team acted swiftly to contain the intrusion. We believe we were successful in doing so within hours after learning of this threat. However, the malware may have resulted in the capture of some kiosk users' personal information, including names and credit and debit card information. I want to stress that contrary to early concerns, no biometric information was captured by the malware. The fingerprint scans used with the U.are.U4500 fingerprint scanner supplied by Avanti Markets are all encrypted and were not vulnerable to this intrusion.

We apologize for any stress and anxiety this incident is causing some of our operators' and their customers. The security of your personal information is our top priority. Please know that we are doing everything in our power to address this problem and to make sure that it will not happen again. It is important to note that the malware affected only a small portion of our kiosks. At the time of this incident, Avanti Markets had delivered updated payment devices that included encryption technology, operators were in the process of deploying to all kiosks. We expect this to be completed by the end of July.

In the meantime, we are committed to providing our operators and consumers with a secure system. Our company has hired an outside law firm and industry leader in cyber technology to perform a root cause analysis. We are determined to learn from this experience and continue to be a leader in the micro market industry.

We have provided the facts as we now know them and the steps we have taken to address this problem. We have also posted detailed information on our website (http://www.avantimarkets.com/notice-of-data-breach/) and contacts for people who have questions and concerns.

We will continue to update you as more information becomes available. Thank you for your understanding and continued support.

- Jim Brinton, Chief Executive Officer and Founder, Avanti Markets

Notice of Data Breach

What Happened?
On July 4, 2017, we were alerted to an intrusion of sophisticated malware attack which affected kiosks at some Avanti Markets. At this stage, we have determined the attack was not successful on all kiosks and many kiosks have not been adversely affected.

What Information Was Involved?
At this point, it appears the malware was designed to gather certain payment card information including the cardholder's first and last name, credit/debit card number and expiration date. Customers who used their Market Card to make payment may have had their names and email addresses compromised. Many kiosks encrypt credit card information and payment card data on those kiosks would not be subject to this incident.

What We Are Doing?
We have been working nonstop to address this incident, including: commencing an investigation to determine the scope of this incident and attempt to identify those affected; working to secure our information systems, including changing passwords and other related measures; retaining a nationally-recognized forensic investigation firm and outside legal counsel to assist; notifying the FBI; shutting down payment

processing at some locations and are working with our operators to purge impacted systems of any malware from the attack to minimize the risk of a data compromise in the future; developed FAQs to assist affected persons; setting up a call center to answer questions about the incident; and continuing to assess and modify our privacy and data security policies and procedures.

We have also made available credit monitoring services at no cost to those individuals whose personal information has been compromised. Specifically, we have partnered with Equifax® to provide its Credit WatchTM Silver identity theft protection product for one year at no charge to you. If you choose to take advantage of this product, it will provide you with a notification of any changes to your credit information, up to $25,000 Identity Theft Insurance Coverage and access to your credit report. To enroll, you must first call 800-224-8040 to obtain an authorization code and then go to www.myservices.equifax.com/silver, enter your activation code, click submit, and follow the enrollment instructions. You must complete the enrollment process by October 9, 2017. We encourage you to enroll in that service.

What You Can Do.

Even if you utilized your payment card at a kiosk, it does not mean you will be affected by this incident. However, out of an abundance of caution, we recommend that you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

   - **Fraud Alert**. Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a 90 day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your credit file for 90 days.

   - **Security Freeze**. Place a "security freeze" on your credit account. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or internet method made available by the credit reporting agencies. Credit reporting agencies charge a $5 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. In your request, you also must include (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)

   Equifax
   P.O. Box 740256
   Atlanta, GA 30374
   (800) 525-6285
   (877) 478-7625 (report fraud)
   www.equifax.com
   www.fraudalerts.equifax.com

   Experian
   P.O. Box 9554
   Allen, TX 75013
   (888) 397-3742

   www.experian.com/consumer

   TransUnion
   P.O. Box 2000
   Chester, PA 19022
   (800) 888-4213
   (800) 680-7289 (report fraud)
   www.transunion.com

   - **Free Credit Report**. Receive a free copy of your credit report by going to www.annualcreditreport.com.

   - **Watch Bills, Statements and Mailing Lists**. If you aren't already doing so, please pay close attention to all bills; credit-card charges, and bank account statements. Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

2. Contact the Federal Trade Commission ("FTC") either by visiting www.ftc.gov, www.consumer.gov/idtheft, by calling (877) 438-4338, or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

3. If you believe you are a victim of identity theft you should immediately report same to law enforcement and/or your state attorney general.

4. *For Maryland Residents*: Maryland Office of the Attorney General is: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Telephone: (888) 743-0023; website: http://www.oag.state.md.us.

5. *For North Carolina Residents*: North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: www.ncdoj.com/

6. *For Puerto Rico Residents*: The total number of affected individuals is unknown.

7. *For Rhode Island Residents*: Rhode Island Office of the Attorney General is: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; Telephone: (401) 274-4400; website: http://www.riag.ri.gov. The total number of affected individuals is unknown.

8. *For New Mexico Residents*: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf.

For More Information.

If you have questions or concerns you may contact us at 800-224-8040.

SOURCE Avanti Markets

Related Links

http://www.avantimarkets.com

Avanti Markets Data Incident Notification

Notificación de Incidente de Data de Avanti Markets

DATA INCIDENT FAQ'S

Dear Valued Customers,

Avanti Markets deeply values the relationships we have with individuals who utilize kiosks supported by Avanti Markets. This notice is to make you aware of an incident which may have resulted in unauthorized access or acquisition of your personal information and/or payment card data, and to provide you information on steps you can take to protect yourself and minimize the possibility of misuse of your information. We apologize for any inconvenience this may

cause you and assure you we are working diligently to resolve this incident and to ensure that it will not happen again.

WHAT HAPPENED?

On July 4, 2017, we discovered a sophisticated malware attack which affected kiosks at some Avanti Markets. Based on our investigation thus far, and although we have not yet confirmed the root cause of the intrusion, it appears the attackers utilized the malware to gain unauthorized access to customer personal information from some kiosks. Because not all of our kiosks are configured or used the same way, personal information on some kiosks may have been adversely affected, while other kiosks may not have been affected.

WAS MY INFORMATION ACCESSED?

We are currently conducting an extensive IT forensic investigation to determine the extent of the attack, including which kiosks were affected. We have determined at this point that the attack was not successful on all kiosks and many kiosks have not been adversely affected. Additionally, based on our investigation at this time, it appears this malware was only active beginning on July 2, 2017. Accordingly, if you did not utilize a kiosk between July 2, 2017 and July 4, 2017, you were likely not affected by this attack.

WHAT INFORMATION WAS COMPROMISED?

As you know, the kiosks do not collect certain data elements (such as Social Security Number, date of birth, or federal or state identification number) from customers. Accordingly, those elements of personal information were not subject to compromise.

However, for customers that used a payment card to complete a purchase on an infected kiosk, the malware may

have compromised cardholder first and last name, credit/debit card number and expiration date. In an abundance of caution, our original notice advised customers who used their Market Card to make payment that they may have had their names and email addresses compromised, as well as their biometric information if they used the kiosk's biometric verification functionality. We are happy to report that we are now able to confirm *all* kiosk fingerprint readers supplied by Avanti include end-to-end encryption on such biometric data and as such this biometric data would not be subject to this incident as it is encrypted.

WAS BIOMETRIC DATA COMPROMISED?

No. In an abundance of caution, our original notice advised customers who used their Market Card and the kiosk's biometric verification functionality may have had their biometric data compromised. We are happy to report that we are now able to confirm *all* kiosk fingerprint readers supplied by Avanti include end-to-end encryption on such biometric data and as such this biometric data would not be subject to this incident as it is encrypted.

WHAT ARE WE DOING?

We have been working nonstop to address this incident, including taking the following steps.

- Immediately upon discovering that we were a victim of a malware attack, we commenced an investigation to determine the scope of this incident and attempt to identify those affected.
- We worked with our assembled internal response team and took steps to secure our information systems, including changing passwords and other related measures.
- We retained a nationally-recognized forensic investigation firm and outside legal counsel to assist.

- We are notifying the Federal Bureau of Investigation ("FBI") and other law enforcement agencies.
- We have shut down payment processing at some locations and are working with our operators to purge impacted systems of any malware from the attack and take steps to substantially minimize the risk of a data compromise in the future.
- We are developing a set of comprehensive FAQs to assist affected persons with gathering additional information about the incident and additional steps they can take to protect their personal information and identity. We plan to update these FAQs when we discover further information about the nature and scope of the attack.
- We have made available credit monitoring services at no cost to those individuals whose personal information has been compromised. Specifically, we have partnered with Equifax® to provide its Credit WatchTM Silver identity theft protection product for two years at no charge to you. If you choose to take advantage of this product, it will provide you with a notification of any changes to your credit information, up to $25,000 Identity Theft Insurance Coverage and access to your credit report. To enroll, you must first call 800-224-8040 to obtain an authorization code and then follow the enrollment instructions that are located here. You must complete the enrollment process by July 8, 2018.
- We are working on setting up a call center that will be available to answer questions you might have about the incident.
- We treat all personal information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. For instance, we are in the middle of implementing an end to end encryption solution for all of our kiosks and are working on expediting that implementation. Theft of data and similar incidents are difficult to prevent in all instances, however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again.

WHAT YOU CAN DO.

Even if you utilized your payment card at a kiosk, it does not mean you will be affected by this incident. However, out of an abundance of caution, we recommend that you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information: Contact the nationwide credit-reporting agencies as soon as possible to:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

- **FRAUD ALERT**. Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a 90-day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your credit file for 90 days.

- **SECURITY FREEZE**. Place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies. Credit reporting agencies charge a $5 fee to place or remove a security freeze,

unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include (documentation for both the spouse and the victim must be submitted when requesting for the spouse's credit report) (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)

Equifax	Experian
TransUnion	
P.O. Box 740256	P.O. Box 9554
P.O. Box 2000	
Atlanta, GA 30374	Allen, TX 75013
Chester, PA 19022	
(800) 525-6285	(888) 397-3742
(800) 888-4213	
www.equifax.com	www.experian.com/consumer
www.transunion.com	

- **FREE CREDIT REPORT**. Receive a free copy of your credit report by going to annualcreditreport.com.
- **WATCH BILLS, STATEMENTS AND MAILING LISTS**. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for

checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it. Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

2. Contact the Federal Trade Commission ("FTC") either by visiting ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

Federal Trade Commission

Consumer Response Center

600 Pennsylvania Avenue

NW Washington, DC 20580

3. If you believe you are a victim of identity theft you should immediately report same to law enforcement and/or your state attorney general.

4. For Maryland Residents: The contact information for the Maryland Office of the Attorney General is: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Telephone: (888) 743-0023; website: http://www.oag.state.md.us.

5. For *North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: ncdoj.com/.

6. For Puerto Rico Residents: The total number of affected individuals is currently unknown.

7. For Rhode Island Residents: The contact information for the Rhode Island Office of the Attorney General is: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; Telephone: (401) 274-4400; website: http://www.riag.ri.gov. The total number of affected individuals is currently unknown.

8. ***ADDITIONAL INFORMATION FOR NEW MEXICO RESIDENTS:*** *You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf*

FOR MORE INFORMATION.

If you have questions or concerns you may contact us by calling 800-224-8040 or emailing **SECURITYINCIDENTINFO@AVANTIMARKETS.COM**. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

JOHN REILLY

PRESIDENT

AVANTI MARKETS

DATA INCIDENT FAQ'S

E-MAIL US

1.888.937.2826

ARE YOU AN OPERATOR?

ORDERS

Privacy Policy

Terms of Service