Representing Management Exclusively in Workplace Law and Related Litigation

jackson | lewis
Attorneys at Law

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

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

JOSEPH J. LAZZAROTTI
EMAIL: LAZZAROTTIJ@JACKSONLEWIS.COM

JASON C. GAVEJIAN
EMAIL: GAVEJIANJ@JACKSONLEWIS.COM

August 30, 2017

VIA ELECTRONIC MAIL
Consumer Protection
800 5th Ave, Suite 2000
Seattle, WA 98104-3188
SecurityBreach@atg.wa.gov.

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

Dear Sir/Madam:

As you know, 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 supplement our correspondence of July 24, 2017 and to update you on the status of our investigation and Avanti Markets' significant remediation efforts.

At this point, it appears the malware was intended to gather certain payment card information including credit/debit card number, expiration date, and CVV code. While our original notice included cardholder name as potentially being compromised, the investigation results have shown this not to be the case. Although 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 providing an update to applicable state agencies of this incident. As the incident did not include card holder names or addresses, we do not anticipate being able to determine the exact number of affected individuals. However, Avanti Markets has worked with its operators and hosts in an effort to provide additional information, including "at risk" time periods for each kiosk as well as redacted card data where applicable. At this stage, it appears the incident may have affected 57,620 individuals. Please note, as Avanti Markets does not maintain address information for potentially affected individuals, it is unable to provide the number of state residents who may have been affected. However, we are able to determine 1,663 individuals utilized a kiosk in your state during the applicable at-risk window. It is Avanti Markets hope that its efforts, including its website notice, state-wide media notice, and communications with its operators, will ensure all those potentially affected by the incident have been made aware.

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

[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.

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. Avanti Markets redoubled its efforts to implement the end-to-end encryption for payment card transactions and as of August 4, 2017, within 30 days of learning of the incident, that solution was installed on 100% of kiosks in the United States. The Company has been working diligently with 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 was implementing the remediation steps outlined above, Avanti Markets also 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 ("FAQs"). Additionally, Avanti Markets provided additional notice via state-wide media through the United States in an effort to reach affected individuals. Since that time, Avanti Markets has provided updates to the website notice, FAQs, and state-wide media notice, to provide customers with up to date information. Avanti Markets intends to continue these efforts as its investigation comes to a conclusion. Copies of the website notice and FAQs are available at: http://www.avantimarkets.com/.

As mentioned above, our original correspondence, and in the applicable 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. 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.

J. Lazzarotti

Joseph J. Lazzarotti
Jason C. Gavejian

Avanti Markets Data Incident Notification

Notificación de Incidente de Data de Avanti Markets

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 continuing to work 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?

Based on our IT forensic investigation, we have determined that the attack was not successful on all kiosks and many kiosks have not been adversely affected. It appears the malware was only active beginning on July 4, 2017. Through a combination of efforts by our incident response team, the number of at-risk kiosks quickly and steadily declined. In the first 14 days of learning of the incident (July 18th) we were able to work with operators and hosts to ensure that the malware that caused the incident was not active on more than 98% of affected kiosks. Shortly after that, by August 4, we completed implementation of end to end encryption on all kiosks in operation throughout the United States, eliminating the risk to payment card transactions on the few remaining kiosks. We are advising anyone who utilized a kiosk between July 4, 2017 and August 4, 2017 (the time period when the malware may have been active) to take steps to protect their information, including enrolling in the credit monitoring service we are providing at no cost to you. However, as noted, during this period the number of at-risk kiosks declined, meaning that not all kiosks were at risk during the entire window. Please note, after ensuring the malware was inactive, we attempted to ascertain the

potential at-risk transactions. Based on that investigation it appears some kiosks may have accepted, but did not complete, a limited number of transactions in the period prior to the date the malware attack began (July 4). These transactions were not completed as the kiosks likely were unable to communicate with the applicable banks when the transactions were attempted. When these kiosks came back online, transactional records suggest that some of the transactions which were attempted, but not processed, may have also been at-risk. Our original notice referenced July 2, 2017, to account for these attempted but not processed transactions. The recent review of the transaction data indicates a very number of transactions which occurred prior to July 2, 2017, may also be at-risk. We learned most of these transactions occurred during the 14-day period prior to July 4, with a very small number of transactions occurring as early as April 7, 2016. To inquire about the remediation date for the kiosk you used, send an inquiry with the address of the kiosk's location
to: securityincidentinfo@avantimarkets.com.

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 results of our investigation show that the malware did not compromise cardholder first or last name but in some cases compromised credit/debit card number, expiration date, and CVV code. While our original notice included cardholder name as

potentially being compromised, the investigation results have shown this not to be the case.

In an abundance of caution, our original notice also advised customers who used their Market Card to make payments 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 notified the Federal Bureau of Investigation ("FBI") and other law enforcement agencies.
- On July 5, we took steps to cease payment processing on affected kiosks and instructed operators on steps to take to minimize the risk of a data compromise in the future which included disabling card readers and posting signage for customers. We redoubled our efforts to implement end to end encryption for payment card transactions on 100% of US kiosks, and completed that on August 4. We additionally worked with operators to purge impacted systems of any malware from the attack.
- We developed 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 will continue to update these FAQs if and/or 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 Watch™ 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.
    - *For Canadian residents, we have made similar monitoring services available, refer to the FAQs for details/instructions.*
- We set up a call center that is available to answer questions you might have about the incident at 800-224-8040.
- 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 have completed the process of implementing end to end encryption for all of our kiosks 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 CAN YOU DO?

The following information is not applicable to Canadian residents.

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 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.

1. 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

1. If you believe you are a victim of identity theft you should immediately report same to law enforcement and/or your state attorney general.
2.

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.

3. *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/.
4. *For Puerto Rico Residents*: The total number of affected individuals is currently unknown.
5. *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.
6. *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

(Updated: 8/29/2017)

E-MAIL US
1.888.937.2826
ARE YOU AN OPERATOR?
ORDERS

© Avanti Markets 2017. All rights reserved.
Privacy Policy
Terms of Service

AVANTI MARKETS DATA INCIDENT FAQ'S

INCIDENT RELATED

WHAT HAPPENED?

The technology and back-end platform that we use to facilitate a 24-hour, self-service marketplace for customers is supported by our technical team and it is serviced and maintained by a network of operators around the country. We believe that sometime shortly before July 4, 2017, the workstation of one of the third party vendor's employees became infected with a sophisticated and malicious malware attack, although our investigation has not enabled us to determine the precise nature of the attack. The malware wound up affecting some kiosks on July 4, 2017. Through a combination of efforts by our incident response team, the number of at risk kiosks quickly and steadily declined. Within hours of learning of this incident on July 4, 2017, we worked with our vendor to take steps to remove the malicious code associated with the malware attack. Within 14 days of

learning of the incident, July 18, we were able to work with operators and hosts to ensure that the malware that caused the incident was not active on more than 98% of affected kiosks. Shortly after that, by August 4, we completed implementation of end to end encryption on all kiosks in operation throughout the United States, eliminating the risk to payment card transactions on the few remaining kiosks. As noted, during these periods the number of at risk kiosks declined, meaning that not all kiosks were at risk during the entire window. To inquire about the remediation date for the kiosk you used, send an inquiry with the address of the kiosk's location to: securityincidentinfo@avantimarkets.com .

WAS MY INFORMATION ACCESSED?

Based on our IT forensic investigation, we have determined that the attack was not successful on all kiosks and many kiosks have not been adversely affected. It appears this malware was only active beginning on July 4, 2017. Through a combination of efforts by our incident response team, the number of at-risk kiosks quickly and steadily declined. In the first 14 days of learning of the incident (July 18th) we were able to work with operators and hosts to ensure that the malware that caused the incident was not active on more than 98% of affected kiosks. Shortly after that, by August 4, we completed implementation of end to end encryption on all kiosks in operation throughout the United States, eliminating the risk to payment card transactions on the few remaining kiosks. For a very small number of kiosks, representing less than 2% of affected kiosks, your information could have been compromised if you used the kiosk between July 19 and August 4. However, on July 5, we provided instructions and took steps to (i) disable card readers and (ii) have notice posted on kiosks alerting customers not to use their payment cards. We are advising

anyone who utilized a kiosk between July 4, 2017 and August 4, 2017 (the time period when the malware may have been active) to take steps to protect their information, including enrolling in the credit monitoring service we are providing at no cost to you. As noted, during this period the number of at-risk kiosks declined, meaning that not all kiosks were at risk during the entire window. Please note, after ensuring the malware was inactive, we attempted to ascertain the potential at-risk transactions. Based on that investigation it appears some kiosks may have accepted, but did not complete, a limited number of transactions in the period prior to the date the malware attack began (July 4). These transactions were not completed as the kiosks likely were unable to communicate with the applicable banks when the transactions were attempted. When these kiosks came back online, transactional records suggest that some of the transactions which were attempted, but not processed, may have also been at-risk. Our original notice referenced July 2, 2017, to account for these attempted but not processed transactions. The recent review of the transaction data indicates a small number of transactions which occurred prior to July 2, 2017, may also be at-risk. We learned most of these transactions occurred during the 14-day period prior to July 4, with a very small number of transactions occurring as early as April 7, 2016. To inquire about the remediation date for the kiosk you used, send an inquiry with the address of the kiosk's location to: securityincidentinfo@avantimarkets.com.

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 credit/debit card number, expiration date, and CVV code. While our original notice included cardholder name as potentially being compromised, the investigation results have shown this not to be the case. In an abundance of caution, our original notice advised customers who used their Market Card to make a 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.

DID THIS ATTACK AFFECT ALL KIOSKS?

No, at this stage, we have determined the attack was not successful on all kiosks and many kiosks have not been adversely affected at all. In May 2017, we began working with our operators to roll out an end-to-end encryption solution to all kiosks. At the time of the incident, the solution had

been installed in more than 50% of kiosks. The payment card information on these kiosks was protected. We believe approximately 2,664, without the end to end encrypted solution at the time of the incident, may have placed credit card information at risk.

HOW DO I KNOW IF THE KIOSK AT MY LOCATION OR THE KIOSK I REGULARLY USE WAS AFFECTED?

As part of our remediation efforts, we have shut down payment card processing at affected kiosk locations. If your kiosk's payment card processing has been disabled or "temporarily unavailable" it is likely that your kiosk was affected by this attack. Please note that even if you used an affected kiosk that does not mean that your personal information was compromised or infiltrated. To inquire about whether your kiosk was affected and the remediation date, send an inquiry with the address of the kiosk's location to: securityincidentinfo@avantimarkets.com.

WHAT IS BEING DONE TO PROTECT ME?

We have been working nonstop to address this incident, remediate the attack and mitigate harm. Immediately upon discovering that our third party vendor was the victim of a malware attack, we worked with our technical team to commence an investigation to determine the scope of this incident and attempt to identify those affected, which included retaining a nationally recognized forensic investigation firm. We worked with our assembled internal response team and took steps to secure our information systems, including taking steps to shut down payment card processing at kiosk locations we believe have been affected and advising all our operators on steps to take to minimize the risk of a data compromise in the future. Within hours of learning of this incident, we worked with our technical team to remove the malicious code associated with the malware

attack and preliminary testing indicates these efforts prohibited any further improper access. We also are continuing to work with our technical team and our operators to ensure all systems have been purged of any malware from the attack including taking steps to substantially minimize the risk of a data compromise in the future.

Within only a few days after our discovering the incident, we published detailed information to help affected individuals learn about steps they could take to safeguard their personal information and protect against identity theft. We also developed these FAQs to provide additional information and assist you with gathering information about the incident as well as additional steps you can take to protect yourself. Finally, 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 two distinct offerings:

- *For U.S. Residents:* We have partnered with Equifax to provide its Credit Watch™ 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 encourage you to enroll in that service.
- *For Canadian Residents*: We have partnered with Equifax to provide its Complete™ Advantage Plan to you for two years at no charge to you. If you choose to take advantage of this product, you can:
    - Monitor your credit. With regular reports and access to your Equifax credit score to notify you of unexpected changes.

- Work with a dedicated Customer Care Representative. Who will answer your questions.
- Help protect your information. Help protect against theft of your social insurance number bank accounts, home and work addresses, and credit and banking history.
- Help reduce financial risk. With up to $25,000 identity theft insurance.

To enroll, you must first call 800-871-0937 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 encourage you to enroll in that service.

WHO IS RESPONSIBLE FOR THIS ATTACK?

We are working with our IT forensic investigators and law enforcement in an effort to determine those responsible. At this time, the responsible party or parties have not been identified.

I AM UPSET MY INFORMATION MAY BE SUBJECT TO THIS ATTACK.

We understand. We apologize for any inconvenience this incident may cause you and assure you were are doing everything we can to help. We have been working nonstop to address this incident, remediate the attack and mitigate harm. Immediately upon discovering that our third party vendor was the victim of a malware attack, we commenced an investigation to determine the scope of this incident and attempt to identify those affected, which included retaining a nationally recognized forensic investigation firm. We worked with our assembled internal response team and took steps to secure our information systems, including taking steps to shut down payment card processing at kiosk locations we believe have been affected and advised all our operators on steps to take to minimize the risk of a data compromise in the future. Within 14 days of learning of the incident, by July

18, we were able to work with operators and hosts to ensure that the malware that caused the incident was not active on more than 98% of affected kiosks. Shortly after that, by August 4, we completed implementation of end to end encryption on all kiosks in operation throughout the United States, eliminating the risk to payment card transactions on the few remaining kiosks. We also are continuing to work with our technical team and our operators to ensure all systems have been purged of any malware from the attack including taking steps to substantially minimize the risk of a data compromise in the future.

Within only a few days after our discovering the incident, we published detailed information to help affected individuals learn about steps they could take to safeguard their personal information and protect against identity theft. We also developed these FAQs to provide additional information and assist you with gathering information about the incident as well as additional steps you can take to protect yourself. Finally, 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 two distinct offerings:

- *For U.S. Residents:* We have partnered with Equifax to provide its Credit Watch™ 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 encourage you to enroll in that service.
- *For Canadian Residents*: We have partnered with Equifax to provide its Complete™ Advantage Plan to you for two years at no

charge to you. If you choose to take advantage of this product, you can:

- Monitor your credit. With regular reports and access to your Equifax credit score to notify you of unexpected changes.
- Work with a dedicated Customer Care Representative who will answer your questions.
- Help protect your information. Help protect against theft of your social insurance number bank accounts, home and work addresses, and credit and banking history.
- Help reduce financial risk. With up to $25,000 identity theft insurance.

- To enroll, you must first call 800-871-0937 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 encourage you to enroll in that service.

ARE THE PEOPLE WHOSE DATA MAY HAVE BEEN COMPROMISED AT RISK FOR IDENTITY THEFT?

Any person who has personal information compromised does have an increased risk of identity theft. We are taking a number of steps to help you minimize the chance of identity theft. This includes enrolling in the credit monitoring service as described above.

SHOULD I BE CALLING MY BANK AND CLOSING MY ACCOUNT? SHOULD I BE CANCELING MY CREDIT CARDS?

Of course, you can take these steps if you feel more comfortable. But, you do not have to close your bank and credit card accounts. Be sure, though, to monitor your bank and credit card statements for accuracy. If you notice any suspicious activity or you believe your information is being misused, please file a report with your local police department and the Federal Trade Commission. You can also enroll in the credit monitoring service as described above.

IS MY SPOUSE/DEPENDENT AFFECTED?

We have no information at this point to suggest that the information of your spouse/child/dependent has been affected by this incident. Please note if they also utilized a payment card at a kiosk during the applicable time period (See "**WAS MY INFORMATION ACCESSED?**" above) they also may have been affected by this incident.

WHEN DID THIS EVENT OCCUR?

We discovered the incident on July 4, 2017. At this stage of our investigation, it appears the malicious malware attack began on July 4, 2017.

WHY DIDN'T YOU TELL ME SOONER?

We believe we acted very quickly to make information available to you following our discovery on July 4, 2017. Our initial website posting was published three (3) days later. These comprehensive FAQs were added a few days after that. However, we have been conducting an extensive internal investigation to understand what happened and what information may have been compromised. This includes coordinating with our technical team, as well our operators. In addition, we needed to retain an IT forensic investigation expert and prepare a process for responding to your follow-up inquiries. We also have been taking extensive steps to remediate any harm and ensure the kiosks are secure. Within 14 days of learning of the incident, by July 18, we were able to work with operators and hosts to ensure that the malware that caused the incident was not active on more than 98% of affected kiosks. Shortly after that, by August 4, we completed implementation of end to end encryption on all kiosks in operation throughout the United States, eliminating the risk to payment card transactions on the few remaining kiosks.

WHAT CAN I DO ON MY OWN TO ADDRESS THIS SITUATION?

There are a number of steps you can take, many of which were detailed in the Customer Notification These include placing a fraud alert with the credit bureaus, reviewing your financial statements, and signing up for credit monitoring.

I RECEIVED AN EMAIL FROM AVANTI REGARDING THIS INCIDENT. IS THIS LEGITIMATE?

In limited instances, we will endeavor to provide notification to potentially affected individuals via email (if we have a valid email address), as well as responding to emails you may have initiated with us. However, you should be aware of scam email campaigns related to this incident. These scams, designed to capture personal information (known as "phishing") are designed to appear as if they are from Avanti and the emails may include a "click here" link or ask you to "open" an attachment. These emails are NOT from us.

- DO NOT click on any links in email.
- DO NOT reply to the email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open, if you have clicked on a link in email.
- DO NOT open any attachments that arrive with email.

Individuals who have provided e-mails to us may receive an e-mail directing them to visit our website for additional information and/or to sign up for credit monitoring. Any such email will not include attachments, embedded links, or in any way ask for personal information.

I RECEIVED A CALL FROM AVANTI REGARDING THIS INCIDENT AND ASKING FOR MY INFORMATION. IS THIS LEGITIMATE?

No. We are NOT calling individuals regarding this incident and are not asking for any of your personal information over the phone.

ORGANIZATION RELATED

HOW CAN I BE SURE THAT MY PERSONAL DATA WON'T BE SUBJECT TO ATTACK AGAIN IN THE FUTURE?

We are doing everything we can to ensure there is no further vulnerability to the kiosks. In May 2017, before the incident occurred, we began working with our technical team and our operators to roll out an end-to-end encryption solution to all kiosks. At the time of the incident, the solution had been installed in more than 50% of kiosks. As of August 4, 2017, within 30 days of learning of the incident, we can now report the solution has been installed in 100% of kiosks in the United States.

We presently are working with a nationally recognized IT forensic investigation firm to investigate this attack and identify additional safeguards which may be utilized to secure data. We comply with federal and state privacy laws and work hard to maintain your personal data in a safe and secure environment. This includes redoubling our efforts to expedite the rollout of our end-to-end encryption solution to all kiosks. Additionally, within hours of learning of this incident, we worked with our technical team to take steps to remove the malicious code associated with the malware attack. We also have been updating all Antivirus Protocols and SW patching, and are continually scanning the network for anomalies. We take data privacy and security very seriously and are continuing to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. However, no set of safeguards is perfect or impenetrable.

WHY DO KIOSKS HAVE MY INFORMATION?

It is necessary for the kiosks to have certain data from customers as part of the point of sale process. However, we

continually work to minimize, to the extent possible, the amount of personal information that needs to be collected and maintained. For instance, in May 2017, before the incident occurred, we began working with our technical team and our operators to roll out an end-to-end encryption solution to all kiosks. At the time of the incident, the solution had been installed in more than 50% of kiosks. This solution would eliminate the storage of payment card data on the kiosks. We are happy to report that as of August 4, 2017, the solution had been installed in 100% of kiosks in the United States.

I AM CONCERNED ABOUT IDENTITY THEFT – WHAT CAN I DO?

There are a variety of steps you can take, many of which are detailed in the Customer Notification and in the FAQs below. These include placing a fraud alert with the credit bureaus, reviewing your financial statements, and signing up for credit monitoring.

IS AVANTI DOING ANYTHING TO HELP ME?

Avanti has endeavored to provide notice of this attack as soon as possible. In addition, we

- have made available to you at no cost a credit monitoring service which is described above in the FAQs below.
- have taken steps to ensure that our electronic systems continue to be secure,
- have notified various third party consultants, IT forensic investigators, and legal counsel to mitigate any possible harm to the extent reasonably possible,
- have notified applicable law enforcement agencies,
- will continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring, including redoubling our efforts to ensure our third party service providers maintain adequate data security.

WAS MY HOME ADDRESS INCLUDED WITH THE INFORMATION AND AM I IN ANY DANGER OF BEING ROBBED?

Your home address information was not included. For perspective, your address is likely available through many other sources of public records and is not generally considered sensitive personal information by itself.

IF MY IDENTITY IS STOLEN, OR IF I AM SUBJECT TO AN INCIDENT OF PAYMENT CARD FRAUD, WILL YOU NOTIFY ME WHEN IT HAPPENS?

By checking your credit report and ensuring you have placed a fraud alert to the three major credit bureaus you are taking the steps to limit your risk of becoming a victim of identity theft. By being proactive with receiving timely credit reports, monitoring your bank and credit card statements, you will be able to notice any inaccuracies as they occur.

IDENTITY THEFT-GENERAL

WHAT IS IDENTITY THEFT?

Identity theft is the taking of the victim's identity to obtain credit, credit cards from banks and retailers, steal money from existing accounts, apply for loans, rent an apartment, file bankruptcy or obtain medical services. Often the victim does not become aware of the crime until months or years after the theft occurs.

WHAT DO I DO NOW? WHAT CAN I DO TO PROTECT MYSELF? HOW DO I FILE A FRAUD ALERT AND GET A COPY OF MY CREDIT REPORT? WHAT ABOUT A SECURITY FREEZE?

There are some simple steps you can take to protect yourself against identity theft or other fraudulent misuses of information about you. Notably, watch for any unusual activity on your credit card accounts or suspicious items on

your bills. You may wish to contact your credit card issuers and inform them of what has taken place. You may also wish to do the following:

- Enroll in the credit monitoring service we are making available to you at no cost.
- Under federal law, you are entitled to one free copy every 12 months of your credit report from each of the three major credit reporting companies. You may obtain a free copy of your credit report by going on the Internet to www.annualcreditreport.com or by calling 1-877-FACTACT (1-877-322-8228). If you would rather write, a request form is available on AnnualCreditReport.com. You may want to obtain copies of your credit reports to ensure the accuracy of the report information.
- When you receive your credit reports, look them over carefully. Look for accounts that you did not open or inquiries from creditors that you did not initiate. Look for personal information that is not accurate. Even if you do not find suspicious activity on your initial credit reports, it is recommended that you check your credit reports every three months for the next year. Checking your reports periodically can help you spot problems and address them.
- To further protect yourself, you may contact the fraud departments of the three major credit reporting companies. They will discuss your options with you. You have the right to ask that these companies place "fraud alerts" in your file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting companies. As soon as that company processes your fraud alert, it will notify the other two credit reporting companies, which must then also place fraud alerts in your file. Contact information for the three major credit reporting companies is provided in the Customer Notification.
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months by visiting com.;

- Review all of your bank account statements frequently for checks, purchases or deductions not made by you;
- If you suspect or know that you are the victim of identity theft, you should contact local police and you also can report this to the Fraud Department of the FTC;
- To place a security freeze on your credit report, y*ou will need to call all three credit bureaus (information listed below). Charges to place and/or remove a security freeze vary by state and credit agency. To place a security freeze, contact:*
- *Equifax 1-800-685-1111*

https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

- *Experian 1-888-397-3742*

http://www.experian.com/consumer/security_freeze.html

- *TransUnion 1-800-680-7289*

http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

WHAT SHOULD I DO IF I NOTICE ANY SUSPICIOUS ACTIVITY ON MY CREDIT REPORT OR MY BANK/CREDIT CARD STATEMENTS?

There are a few steps you must take. Call one of the 3 credit bureaus to:

- Declare yourself an identity theft victim
- Request a free credit report
- Ask that a fraud alert be placed on your credit file
- And, ask that bureau to contact the remaining 2 credit bureaus to request fraud alerts on your file.
- Contact for the three major credit reporting companies is provided in the Customer Notification.

While you may experience wait times of similar difficulties when contacting the credit bureaus, be persistent and begin

monitoring your financial statements and contacting the institutions with suspected fraudulent activities. You may want to visit each of the credit bureau's websites to place fraud alerts on your accounts, but we recommend calling the toll-free number.

Second, filing a complaint with the police is required by many institutions to prove that your identity was stolen. After filing the complaint, you should ask for a copy of the police report because you will need to attach this report to all written correspondence sent in your effort to resolve any fraudulent activities. Be polite, but persistent with the police because in many areas they are understaffed to deal efficiently with your identity theft.

WHAT SHOULD I DO IF THE LOCAL POLICE WILL NOT TAKE A REPORT FROM ME?

There are efforts at the federal, state and local level to ensure that local law enforcement agencies understand identity theft, its impact on victims, and the importance of taking a police report. However, we still hear that some departments are not taking reports. The following tips may help you to get a report if you're having difficulties:

- Furnish as much documentation as you can to prove your case. Debt collection
  letters, credit reports, and other evidence of fraudulent activity can help demonstrate the seriousness of your case.
- Be persistent if local authorities tell you that they can't take a report. Stress the
  importance of a police report; many creditors require one to resolve your dispute.
  Remind them that credit bureaus will automatically block the fraudulent accounts
  and bad debts from appearing on your credit report, but only if you can give them
  a copy of the police report.

- If you're told that identity theft is not a crime under your state law, ask to file a
  Miscellaneous Incident Report instead.
- If you can't get the local police to take a report, try your county police. If that
  doesn't work, try your state police.
- Some states require the police to take reports for identity theft. Check with the
  office of your State Attorney General to find out if your state has this law.LINK TO ALL STATE ATTORNEY GENERAL OFFICES:

http://www.privacycouncil.com/id_theft_resources.php

WHAT ARE TYPICAL THINGS THAT AN IDENTITY THIEF WOULD DO?

Identity thieves have been known to take a victim's identity to obtain credit, credit cards from banks and retailers, steal money from existing accounts, apply for loans, rent an apartment, file bankruptcy or obtain medical services.

WHAT IS A FRAUD ALERT AND HOW LONG DOES IT LAST?

A Fraud Alert is a flag that the credit reporting agencies put in your file to instruct creditors to take extra precautions, such as additional verification of your identity when opening accounts or issuing credit. An initial fraud alert lasts 90 days. An extended alert lasts for 7 years.

WHY SHOULD I SET A FRAUD ALERT WITH THE CREDIT BUREAUS?

This will prevent someone from opening new accounts in your name. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts as well. All three bureaus will place a message on your report that tells creditors to call you before opening any new accounts.

You will not be charged for this service. Please note, placing a fraud alert may delay your ability to open new lines of credit

quickly. You should notify any new creditors with whom you have applied that you have a fraud alert placed.

WHEN A FRAUD ALERT HAS BEEN SET, WILL IT TRIGGER AN AUTOMATIC MAILING OF A CREDIT REPORT?

It is recommended that you request your free credit reports before setting a fraud alert. If you do not, about one week after setting the fraud alert, you will receive confirmation letters from the credit bureaus. These letters will explain that you have to call each bureau and order your free report. They will provide the phone numbers you need to call. Once you call and order, your report should arrive within 2 weeks in a plain, unmarked envelope. Be sure to examine it carefully. You are entitled to one free copy for every 90 day alert period.

I ALREADY PLACED FRAUD ALERTS. CAN I PLACE THEM AGAIN?

The fraud alerts last 90 days and the system will let you know the alerts are already in place if you try to place them again before they expire. There is no penalty for doing this. You will NOT be notified when fraud alerts expire, so note the date and you can place them every 90 days for as long as you wish.

CREDIT REPORTS

HOW DO I GET A FREE COPY OF MY CREDIT REPORT?

Under federal law, you are entitled to one free copy of your credit report every twelve months from each of the three major credit reporting companies. You may obtain a free copy of your credit report by going on the internet to www.AnnualCreditReport.com or by calling 1-877-FACTACT (1-877-322-8228). If you would rather write, a request form is available on www.AnnualCreditReport.com. You may want to

obtain copies of your credit reports to ensure the accuracy of the report information.

WHAT DO I DO IF THERE IS INFORMATION ON MY CREDIT REPORT THAT IS OLD/INACCURATE?

Very often, a credit report will contain information that is a result of human error (typos, reporting errors or inaccuracies, outdated information). Sometimes, even social security number variations can appear. This is usually not identity theft, and it is up to the individual to dispute the incorrect information with the credit bureaus. Call the number provided on your report.

However, if you discover this information along with other evidence of fraud (new accounts, collections accounts that aren't yours, etc.), you may be a victim of identity theft. It is best to begin by contacting the bureau to find out why/how the information is being reported. You can begin disputes with them. (See other FAQs below to get answers about disputing fraudulent accounts)

WHAT SHOULD I LOOK FOR ON A CREDIT REPORT TO INDICATE IDENTITY THEFT?

Accounts

Look for accounts you didn't open and unexplained debts or authorized users that you didn't authorize on your legitimate accounts.

Personal Information

Check to see if your personal information (your SSN; address (es); name and any
variations, including initials, Jr., Sr., etc.; telephone number(s); and employers) are correct. Inaccuracies in this information may also be due to typographical errors. If you believe that the inaccuracies are due to error, you should notify the credit

bureaus by telephone and/or in writing to dispute the information.

Inquiries

Inquiries on credit reports from potential credit card issuers do not always mean that someone has tried to get credit in your name. Banks and credit card companies often inquire about a consumer's creditworthiness to help them target their marketing efforts.

These inquiries will be identified in a designated section of the report and are described as "Inquiries that are viewed by others and don't affect your credit score." If you would not like your information to be used in this way, you can call 1-800-5 OPT OUT (1-800- 567-8688). You are automatically opted-out of data sharing when you place fraud alerts.

Inquiries that are described as displaying to others and affecting your credit score are the ones you need to be concerned with—these appear when someone has applied for credit in your name.

GENERAL CREDIT MONITORING QUESTIONS

I KEEP SEEING "CREDIT MONITORING" OFFERED ON THE BUREAU'S WEBSITES. WHAT IS CREDIT MONITORING?

Monitoring your credit reports regularly is a helpful way to detect and prevent fraud. Credit monitoring assists you with this process. Each of the bureaus offers some kind of credit monitoring service that you can purchase. Remember, we will be making credit monitoring available to you at no cost. The enrollment process in described in the Customer Notification on the website. The options are usually to monitor only one of your reports or all three. Some other Internet companies and financial institutions offer a monitoring service as well. We suggest you research the service and the company very

well before purchasing the monitoring to ensure it is a reliable product.

The way monitoring works is that every week, you are informed of any changes to your credit report. You'll be alerted to what's happening with your credit by knowing about the following changes (all of which could indicate fraud):

- New inquiries
- New accounts opened in your name
- Late payments
- Improvements in your report
- Bankruptcies and other public records
- New addresses
- New employers

SHOULD I BUY CREDIT MONITORING?

That is a decision that we recommend each person make for herself/himself. Please note, however, Avanti is making available a monitoring service for you at no cost. The enrollment process is described in the Customer Notification on the website.

CAN YOU ENROLL ME IN CREDIT MONITORING?

No, we cannot. This is something you will have to do individually.

IF I CHOOSE TO PURCHASE CREDIT MONITORING AND REPAIR SERVICES, WILL YOU REIMBURSE ME?

No. We will be contracting with a trusted vendor to provide monitoring services at no cost to you and will not reimburse for services that may have been independently purchased.

I LIVE IN CANADA, HOW CAN I CONTACT EQUIFAX IN CANADA?

Equifax in Canada can be reached at 1-800-871-3250 or 1-877-493-8785.

(Updated: 8/29/17)

4848-8382-2925, v. 1

(Updated: 8/29/17)

E-MAIL US
1.888.937.2826
ARE YOU AN OPERATOR?
ORDERS

© Avanti Markets 2017. All rights reserved.
Privacy Policy
Terms of Service