ABM Parking Services Inc. Provides Public Notice Of Vendor's Data Security Incident At Nine Chicago Parking Lots

December 5, 2014

Notice for Massachusetts residents

CHICAGO, IL - December 5, 2014 - ABM Parking Services, Inc. ("the company"), today announced that Datapark USA Inc. a vendor that provides and maintains point of service software for several Chicago, Illinois parking facilities managed by the company, has confirmed a data security incident. This incident may involve certain customer credit and debit card information, including payment card numbers.

After being notified by Datapark of a potential compromise, the company launched an investigation to: confirm the nature of any unauthorized access to its system; identify any information that may have been exposed; and quickly remediate the compromise. The company engaged independent data forensic experts to assist with the investigation. At this time, the company believes the following Chicago locations were affected during the indicated dates:

- 130 E. Randolph St., Chicago IL 60601 (9/29/14 - 11/1/14)
- 1 South Wacker Dr., Chicago, IL 60606 (9/30/14 - 10/30/14)
- 225 W. Wacker Dr., Chicago IL 60606 (9/29/14 - 10/31/14)
- 303 E. Wacker Dr., Chicago IL 60601 (9/29/14 - 10/31/14)
- 55 East Jackson Blvd., Chicago IL 60604 (9/30/14 - 10/31/14)
- 60 E. Randolph St., Chicago, IL. 60601 (10/6/14 - 10/31/14)
- 227 W. Monroe St., Chicago IL 60606 (9/30/14 - 10/31/14)
- 10-30 South Wacker Dr., Chicago IL 60606 (9/29/14 - 11/6/14)
- 111 E. Wacker Dr., Chicago IL 60601 (9/29/14 - 11/1/14)

The company encourages customers who used payment cards (i.e., credit or debit cards) for transactions on the dates noted at these locations to review their payment card statements for signs of unusual activity. Datapark has indicated that it has "blocked access to prevent any further unauthorized entry into the[ir] servers." The forensic evidence indicates that the compromise was limited to payment card data and that no other personally identifiable information was exposed. Law enforcement and the credit card brands have been notified of this incident.

A toll-free information line is available for customers at (877) 238-3790. To help protect your identity and credit card information, ABM is offering all affected individuals a complimentary one-year membership of Experian's® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. You may enroll by calling (877) 238-3790.

The company encourages customers to remain vigilant and seek to protect against possible misuse of credit cards, identity theft, or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, (877) 322-8228.

At no charge, customers can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, a fraud alert may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/bcp/edu/microsites/idtheft/ or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. State Attorneys General may also have advice on preventing identity theft, and instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, http://www.oag.state.md.us.

Contact

Media/ABM:
Chas Strong
770.953.5072
chas.strong@abm.com