

TJ Maxx hit by hackers; consumerâ€™s credit, debit cards at risk

by Bend Weekly News Sources

The TJX Companies, Inc., parent company to TJ Maxx and Marshalls, yesterday announced that it has suffered an "unauthorized intrusion" into its computer systems that process and store information related to customer transactions. Thieves may have been clandestinely stealing private data for up to three years before their actions were detected in mid-December.

The company has 2,500 storefronts which includes the Bend, Oregon TJ Maxx outlet, a 28,000 square-foot store that celebrated its grand opening in the Bend River Promenade in May 2006. TJX would not say exactly how many customers may be affected, only that they have "specifically identified some customer information that has been stolen" from its systems. Potentially millions of customers may be impacted, experts said.

The breach involves the portion credit card, debit card, check, and merchandise return transactions for customers of its T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and Puerto Rico, and its Winners and HomeSense stores in Canada. It may also involve customers of its T.K. Maxx stores in the U.K. and Ireland, and extend to TJXâ€™s Bobâ€™s Stores in the U.S.

The Company immediately alerted law enforcement authorities of the crime and is working with them to help identify those responsible. TJX is also cooperating with credit and debit card issuers and providing them with information on the intrusion.

TJX is conducting a full investigation of the intrusion with the assistance of several leading computer security and incident response firms and is seeking to determine what customer information may have been compromised.

Since the intrusion, TJX has strengthened the security of its computer systems. While no computer security can completely guarantee the safety of data, the experts working for the company say the containment plan is appropriate to prevent future intrusions and to protect the safety of credit card, debit card and other customer transactions in its stores.

Ben Cammarata, Chairman and Acting Chief Executive Officer of The TJX Companies, Inc., stated, "We are deeply concerned about this event and the difficulties it may cause our customers. Since discovering this crime, we have been working diligently to further protect our customers and strengthen the security of our computer systems and we believe customers should feel safe shopping in our stores. Our first

concern is the potential impact of this crime on our customers, and we strongly recommend that they carefully review their credit card and debit card statements and other account information for unauthorized use. We want to assure our customers that this issue has the highest priority at TJX.â€•

Important Information for Customers

â€¢ TJX has established a special helpline for its customers who have questions about this situation. Customers may reach the helpline toll-free at 866-484-6978 in the United States, 866-903-1408 in Canada, and 0800 77 90 15 in the United Kingdom and Ireland.

â€¢ TJX will also provide information for customers on its website, www.tjx.com, including tips on preventing credit and debit card fraud and other steps customers may take to protect their personal information.

â€¢ TJX strongly recommends that customers carefully review their account statements and immediately notify their credit or debit card company or bank if they suspect fraudulent use.

Actions Taken By TJX

â€¢ Upon discovery of the intrusion in mid-December, 2006, TJX immediately notified and began working closely with law enforcement authorities, including the United States Department of Justice and Secret Service and the Royal Canadian Mounted Police. The Company has coordinated its actions with these authorities and provided all assistance requested to seek to identify the criminals responsible for this incident. TJX maintained the confidentiality of this intrusion as requested by law enforcement.

â€¢ The Company immediately engaged General Dynamics Corporation and IBM Corporation, two leading computer security and incident response firms. TJX has been working aggressively with these firms to monitor and evaluate the intrusion, assess possible data compromise, and seek to identify affected information. These firms have assisted TJX in further securing its computer systems and implementing security upgrades.

â€¢ TJX promptly notified and began working closely with the major credit card companies (American Express, Discover, MasterCard and VISA) and entities that process our customers' transactions. The Company has been providing them information including all requested credit and debit card information.

Information About the Intrusion

Through its investigation, TJX has learned the following with respect to the intrusion:

• An unauthorized intruder accessed TJX's computer systems that process and store information related to customer transactions for its T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and Puerto Rico and its Winners and HomeSense stores in Canada.

• The Company is concerned that the intrusion may extend to the computer systems that process and store information related to customer transactions for T.K. Maxx in the U.K. and Ireland, although TJX's investigation has not yet been able to confirm any such intrusion. It is possible that the intrusion may extend to Bob's Stores.

• Portions of the information stored in the affected part of TJX's network regarding credit and debit card sales transactions in TJX's stores (excluding Bob's Stores) in the U.S., Canada, and Puerto Rico during 2003, as well as such information for these stores for the period from mid-May through December, 2006 may have been accessed in the intrusion. TJX has provided the credit card companies and issuing banks with information on these and other transactions.

• To date, TJX has been able to specifically identify a limited number of credit card and debit card holders whose information was removed from its system and is providing this information to the credit card companies. In addition, TJX has been able to specifically identify a relatively small number of customer names with related drivers' license numbers that were also removed from its system, and TJX is contacting these individuals directly.

• TJX is continuing its investigation seeking to determine whether additional customer information may have been compromised. TJX does not know if it will be able to identify additional information of specific customers that may have been taken.

The Company does not yet have enough information to estimate the extent of the financial cost it will incur as a result of this situation, and does not expect to be able to quantify the estimated financial impact of this issue at the time TJX announces January 2007 sales.

The TJX Companies, Inc. is an off-price retailer of apparel and home fashions. The Company operates 826 T.J. Maxx, 751 Marshalls, 271 HomeGoods, and 162 A.J. Wright stores, as well as 36 Bob's Stores, in the United States. In Canada, the Company operates 184 Winners and 68 HomeSense stores, and in Europe, 212 T.K. Maxx stores.

TJ Maxx hit by hackers; consumerâ€™s credit, debit cards at risk by Bend Weekly News Sources