



NEWS RELEASE

CONTACT:

Sherry Lang
Senior Vice President,
Investor and Public Relations
(508) 390-2323

FOR IMMEDIATE RELEASE

Wednesday, February 21, 2007

THE TJX COMPANIES, INC. UPDATES INFORMATION ON COMPUTER SYSTEMS INTRUSION

Framingham, MA -- The TJX Companies, Inc. (NYSE: TJX), the leading off-price retailer of apparel and home fashions in the U.S. and worldwide, today reported its updated findings from the Company's ongoing investigation of its previously announced unauthorized intrusion into its computer systems.

Carol Meyrowitz, President and Chief Executive Officer of The TJX Companies, commented, "Let me begin by telling our customers personally how much I regret any problems or inconvenience they may have experienced as a result of the unauthorized intrusion into our computer system. Our investigation is ongoing, and we are providing an update today on new developments. We are dedicating substantial resources to investigating and evaluating the intrusion which, given the nature of the breach, the size and international scope of our operations, and the complexity of the way credit card transactions are processed, is, by necessity, taking time. We have a very large team of people working on the investigation. For example, the leading computer security experts working with us have over 50 experts committed to this project. Additionally, with their help, we have strengthened the security of our computer systems. Based on everything we have done, I believe customers should feel safe shopping in our stores. We value our customers' trust and I want our customers to know that I am deeply committed to continuing to address the security of our computer systems, and that TJX will provide periodic updates as we learn more."

The following are new findings based on TJX's current information from its ongoing investigation of the previously announced unauthorized intrusion into its computer system:

Timing

While the Company previously believed that the intrusion took place only from May 2006 to January 2007, TJX now believes its computer system was also intruded upon in July 2005 and on various subsequent dates in 2005. TJX continues to believe there was no compromise of customer data after mid-December 2006.

Credit and Debit Card Data

In addition to the customer data the Company previously reported as compromised, the Company now believes that information regarding portions of the credit and debit card transactions at its U.S., Puerto Rican and Canadian stores (excluding debit card transactions with cards issued by Canadian banks) from January 2003 through June 2004 was compromised. The Company had previously reported that the 2003 transaction data had potentially been accessed. For most of the transactions from September 2003 through June 2004, some of the card information was masked at the time of the transaction, making that portion unavailable to the intruder.

Names and addresses were not included with the credit and debit card data believed compromised. Debit card personal identification numbers (PINs), information from transactions at Bob's Stores, and transactions made with debit cards issued by Canadian banks are not believed to have been compromised.

-MORE-

THE TJX COMPANIES, INC. UPDATES INFORMATION ON COMPUTER SYSTEMS INTRUSION

Wednesday, February 21, 2007

Page 2

Drivers' License Numbers

TJX has found additional drivers' license numbers together with related names and addresses that it believes were compromised. This information was associated with unreceipted merchandise returns at its T.J. Maxx, Marshalls, and HomeGoods stores in the U.S. and Puerto Rico for the last four months of 2003 and May and June 2004. TJX intends to notify customers it is able to identify whose drivers' license numbers, names and addresses were included in the information believed to have been compromised.

T.K. Maxx

The Company had previously reported that it was concerned that T.K. Maxx customer transactions in the UK and Ireland could be involved. TJX's investigation has found evidence of an intrusion to the portion of its computer system that processes T.K. Maxx customer transactions. While TJX continues to suspect that customer information may have been compromised from this portion of its network, the Company has not been able to confirm any unauthorized access to customer data or any theft of customer data from T.K. Maxx.

Important Information for Customers

- TJX has continued to cooperate with law enforcement since the probability of an intrusion was first confirmed as well as with the credit card companies and banks that process its transactions.
- 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.
- TJX will also provide updated 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.
- 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.

About The TJX Companies, Inc.

The TJX Companies, Inc. is the leading off-price retailer of apparel and home fashions in the U.S. and worldwide. The Company operates 821 T.J. Maxx, 748 Marshalls, 270 HomeGoods, and 129 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, 210 T.K. Maxx stores. TJX's press releases and financial information are also available on the Internet at www.tjx.com.

SAFE HARBOR STATEMENTS UNDER THE PRIVATE SECURITIES LITIGATION REFORM ACT OF 1995: Various statements made in this release are forward-looking and involve a number of risks and uncertainties. All statements that address activities, events or developments that we intend, expect or believe may occur in the future, including projections of earnings per share and same store sales, are forward-looking statements. The following are some of the factors that could cause actual results to differ materially from the forward-looking statements: the results and effects of the intrusion into our computer system including the outcome of our investigation, the extent of customer information compromised and consequences to our business including effects on sales and liabilities and costs in connection with this intrusion; our ability to successfully expand our store base and increase same store sales; risks of expansion and costs of contraction; our ability to successfully implement our opportunistic inventory strategies and to effectively manage our inventories; successful advertising and promotion; consumer confidence, demand, spending habits and buying preferences; effects of unseasonable weather; competitive factors; factors affecting availability of store and distribution center locations on suitable terms; factors affecting our recruitment and employment of associates; factors affecting expenses; success of our acquisition and divestiture activities; our ability to successfully implement technologies and systems and protect data; our ability to continue to generate adequate cash flows; our ability to execute the share repurchase program; availability and cost of financing; general economic conditions, including gasoline prices; potential disruptions due to wars, natural disasters and other events beyond our control; changes in currency and exchange rates; import risks; adverse outcomes for any significant litigation; changes in laws and regulations and accounting rules and principles; adequacy of reserves; closing adjustments; effectiveness of internal controls; and other factors that may be described in our filings with the Securities and Exchange Commission. We do not undertake to publicly update or revise our forward-looking statements even if experience or future changes make it clear that any projected results expressed or implied in such statements will not be realized.

-END-