

For Immediate Release:

**DSW Releases Findings from Fraud Investigation into
Credit Card and Other Purchase Information Theft**

COLUMBUS, Ohio – April 18, 2005 – Retail Ventures, Inc. (NYSE: RVI) today issued the findings from its investigation into the theft of credit card and other purchase information from its subsidiary, DSW Shoe Warehouse (DSW). The theft was previously reported in a March 8, 2005 press release. The data stolen was purchase information from DSW customers who shopped at certain DSW stores primarily between mid-November 2004 and mid-February 2005. The key facts reported below were just verified in the forensic investigation by one of the nation's leading computer security firms.

“Our first concern remains our customers,” said Debbie Ferrée, President of DSW. “We believe we have taken the steps needed to alert our customers. While others have guessed as to the extent of the data stolen, DSW waited to report the key facts listed below until we knew what they were and that the forensic investigation verified them as accurate. We also want our customers to know that we have implemented measures to prevent further data theft of this nature.”

Contrary to published reports, DSW has not previously estimated the amount of data stolen.

The key facts as known today are:

- Information from 108 stores was stolen (for a list of stores, go to www.DSWShoe.com). The number of stores was initially thought to be 103.
- Transaction information involving 1.4 million credit cards was obtained. For each card, the stolen information included credit or debit card number, name and transaction amount. Neither addresses nor any other information from the credit card users was stolen, as it was not provided at the point of purchase and, therefore, not stored. (No PIN numbers were among the stolen data.)
- Transaction information involving 96,000 checks was stolen. In these cases, checking account numbers and driver's license numbers were obtained. **Importantly, customer names, addresses and Social Security numbers were not obtained.**
- Customer information provided through the DSW proprietary Reward Your Style Program or via DSW's Web site (www.DSWShoe.com) was not accessed or stolen.

What the company has done:

- **Within 24 hours of discovery of the theft**, contacted federal law enforcement authorities (the United States Attorney's Office and the U.S. Secret Service). These authorities continue to investigate this crime. DSW is providing all requested assistance and working with the authorities to pursue those responsible for this crime and, if apprehended, prosecuting to the fullest extent of the law.
- **Within 24 hours of discovery of the theft**, contacted and brought in a leading computer security firm, Ubizen (owned by a company named Cybertrust Inc.) to begin a forensic investigation. The security firm has confirmed that DSW has taken appropriate steps since the incident to prevent any further data theft.

- **Within 24 hours of discovery of the theft**, notified cardholder associations (VISA, MasterCard, Discover and American Express).
- **Promptly issued** a press release alert and posted a customer alert, as well as information and links pertaining to security issues and the theft of personal information, on www.DSWShoe.com.
- **Provided the stolen credit and debit card numbers to American Express, Discover, VISA and MasterCard.** VISA and MasterCard provided these card numbers to the issuing banks and American Express and Discover implemented their standard procedures to monitor the cards at risk. Again, the addresses of customers who used credit cards were not taken. With additional effort, DSW was able to obtain contact information for approximately half of the affected credit card customers and is in the process of sending notification letters to each of these customers. The letter advises customers to contact their credit card company or issuing bank for further instructions, and directs customers to other helpful resources.
- **With respect to checking account information**, neither the name nor address of customers paying by check is recorded at the time of the purchase. Therefore, additional research was required to determine a way to provide notice, but DSW has now gathered names and addresses for approximately 88 percent of the affected checking account customers and is in the process of sending notification letters to each of these customers. The letter advises customers to contact their bank for further instructions and directs customers to helpful resources. DSW is also in the process of sending letters to the banks of affected accounts.

“We understand that our customers feel violated by this criminal act, and we feel the same,” Ferrée added. “Our sincere apologies go out to our customers for the inconvenience this may have caused. We will continue to work with authorities to identify and prosecute those responsible for this crime to the full extent of the law.”

Anyone who suspects unauthorized use of credit card or checking account information should immediately contact her or his credit card company or bank to notify it of the possible unauthorized transactions.

A posting of the individual stores affected is available at www.DSWShoe.com. This site, www.DSWShoe.com, also contains information on steps to take when checking account and driver’s license information is stolen, how to obtain credit reports and tips on preventing credit card fraud.

DSW operates 176 better-branded DSW stores in major metropolitan areas throughout the country. DSW is a subsidiary of Retail Ventures, Inc.