UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

June 5, 2007

Michael E. Burke, Esq.
Williams Mullen
1666 K Street NW, Suite 1200
Washington, D.C. 20006

Re: Dollar Tree Stores, Inc.

Dear Mr. Burke:

As you know, the Division of Privacy and Identity Protection staff has conducted an investigation into possible violations of Section 5 of the Federal Trade Commission Act by your client, Dollar Tree Stores, Inc. ("Dollar Tree"). According to news reports, unauthorized persons may have obtained personal information, including debit card numbers, of consumers who made purchases at several Dollar Tree stores.[1] The investigation considered whether Dollar Tree engaged in unfair or deceptive acts or practices by failing to provide reasonable and appropriate security for personal information collected at its stores.

Based on our investigation, it appears that, until at least June 2006, Dollar Tree stores were vulnerable to tampering with or theft of their PIN entry devices ("PEDs") by unauthorized individuals attempting to access the personal information provided by consumers to pay for their purchases. In particular, we believe that Dollar Tree stores were vulnerable to a fraudulent practice known as "PED skimming," in which an unauthorized individual uses a device to capture the personal information associated with payment cards when the cards are legitimately used at PEDs located at store check out lanes. As a result, unauthorized persons could tamper with the PEDs in order to capture consumers' personal information, including magnetic stripe data and the PIN associated with a particular card.[2]

Despite these concerns, the staff has determined to close the investigation. Among the factors we considered were the extent to which the risk at issue was reasonably foreseeable at the time of the compromise; the nature and magnitude of the risk relative to other risks; the

---

[1] See, for example, John Ortiz, *Dollar Tree store in data-theft case* (Aug. 2, 2006), The Sacramento Bee, available at http://www.tmcnet.com/usubmit/2006/08/02/1766616.htm.

[2] The PED skimming variant here appears to have involved a sophisticated criminal enterprise: an unauthorized individual apparently dismantled PEDs at several Dollar Tree stores; used a hidden memory chip to secretly capture personal information; and then later returned to the stores, removed (and possibly replaced) the PEDs, and used the information to create counterfeit payment cards.

benefits relative to the costs of protecting against the risk; Dollar Tree's overall data security practices; the duration and scope of the compromise; the level of consumer injury; and Dollar Tree's prompt response to the incident. Applying these factors, the circumstances in this matter contrast significantly with those in recent enforcement actions brought by the Commission. For example, in the Commission's actions against CardSystems Solutions, DSW, ChoicePoint, and BJ's Wholesale Club, we alleged multiple failures to address well-known vulnerabilities; failure to use readily available, and often inexpensive security measures; and substantial injury to consumers in the form of account fraud, time loss, and inconvenience.[3]

We continue to emphasize that data security is an ongoing process, and that as risks, technologies, and circumstances change over time, companies must adjust their information security programs accordingly. The staff notes that, in recent months, the risk of PED skimming at retail locations has been increasingly identified by security experts and discussed in a variety of public and business contexts. We also understand that some businesses have now taken steps to improve physical security to deter PED skimming, such as locking or otherwise securing PEDs in checkout lanes; installing security cameras or other monitoring devices; performing regular PED inspections to detect tampering, theft, or other misuse; and/or replacing older PEDs with newer tamper-resistant and tamper-evident models. We hope and expect that all businesses using PEDs in their stores will consider implementing these and/or other reasonable and appropriate safeguards to secure their systems.

The closing of this investigation is not to be construed as a determination that a violation may not have occurred, just as the pendency of an investigation should not be construed as a determination that a violation has occurred. The Commission reserves the right to take such further action as the public interest may require.

Sincerely,

Joel Winston, Associate Director
Division of Privacy and Identity Protection

---

[3] See http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.