

B&N: PIN pad tampering was "sophisticated" crime

October 24 2012

(AP)—Barnes & Noble Inc. said Wednesday the tampering of devices used by customers to swipe credit and debit cards in 63 of its stores was a "sophisticated criminal effort" to steal information, and reiterated it's working with federal law enforcement authorities.

The largest U.S. bookseller late Tuesday disclosed the data breach in stores in California, Connecticut, Florida, Illinois, Massachusetts, New Jersey, New York, Pennsylvania and Rhode Island, and warned customers to check for unauthorized transactions and to change their personal identification numbers, or PINs.

B&N said only one device, or PIN pad, was tampered with in each store, affecting less than 1 percent of these devices in its stores. It released a complete list of locations that were affected. All the PIN pads in its nearly 700 stores nationwide were disconnected on Sept. 14, after the company learned of the tampering.

In a press release issued Wednesday, B&N said the criminals planted bugs in the tampered devices, allowing for the capture of credit card and PIN numbers. The company did not offer a timeline for when the bugs were planted or how long they were in use before they were discovered.

B&N said that it's continuing to work with federal law enforcement and with banks, payment card brands and issuers to identify accounts that may have been compromised, so that additional fraud-protection measures can be taken.

Customers at its book stores will now have to ask cashiers to swipe credit or debit cards on card readers connected to cash registers, a process that is secure, Barnes & Noble said.

Anything bought on Barnes & Noble.com or with the chain's Nook devices and app were not affected, the company said. It also said its customer database is secure.

Barnes & Noble is only the latest major retailer to be a victim of a serious data breach. In one of the largest, more than 45 million credit and debit cards were exposed to possible fraud because of hackers who broke into the computer system of TJX Cos., the parent company of retailers T.J. Maxx and Marshall's, starting in 2005.

Copyright 2012 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: B&N: PIN pad tampering was "sophisticated" crime (2012, October 24) retrieved 1 July 2024 from <https://phys.org/news/2012-10-bn-pin-pad-tampering-sophisticated.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--