Six New England Banks Alert Customers to Possible Debit Card Data Breach

November 20, 2024 - Six Massachusetts-based regional banks have issued warnings to customers about potential debit card data breaches, advising them to remain vigilant and, in some cases, replacing their cards entirely. The affected banks include Eagle Bank, The Village Bank, Savers Bank, Webster Five, Watertown Savings Bank, and Main Street Bank.

The breach appears linked to a compromised merchant payment network, with unauthorized access to Mastercard debit card details. While The Village Bank confirmed that a credit card skimming device was discovered at a Newton retail establishment, it is unclear whether the same incident affected other banks.

Mastercard has clarified that its systems were not breached. Instead, the issue stems from vulnerabilities in specific merchants' systems where affected customers made transactions. Neither Mastercard nor the banks have disclosed the names of the merchants involved.

Each bank has taken steps to address the breach but their approaches have been inconsistent. Eagle Bank, Savers Bank, and Main Street Bank all automatically replaced customers' debit cards and terminated compromised accounts. But, for instance, Watertown Savings Bank customers were informed that their names and card numbers were accessed. The bank advised monitoring account activity for up to two years and offered to replace debit cards upon request but didnâ€™t do so automatically.

Some of the banks also disclosed varying time frames for when customer data may have been exposed

Although the banks have taken various measures to protect their customers, those affected should remain cautious. Two banks provided contact information for credit bureaus to enable customers to check their credit reports and freeze their credit if necessaryâ€”a step often taken to prevent identity theft.

All customers are advised to monitor their accounts for unusual activity, report discrepancies immediately, and consider placing fraud alerts or credit freezes on their accounts.

While some of the banks have acted swiftly in replacing compromised cards, the lack of detailed information about the breaches and affected merchants raises concerns. Customers are left to speculate about their exposure, highlighting the need for increased transparency. Additionally, only two banks explicitly mentioned credit monitoring or freezing options, leaving some customers without essential guidance.

ACCESS is advising customers of any of these banks to contact them and ask if their information could have been compromised during these data breaches. If the answer is yes, then they should request new debit cards immediately and deactivate any debit cards currently in their possession. Customers of these banks should also look closely at any of their billing statements to make sure there are no erroneous charges on them.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS