The Virgin Islands Consortium

Residents' Debit and Credit Cards Charged Hundreds of Dollars Through Cyber Attack on WAPA Payments Vendor; Customers Urged to Utilize Other Forms of Payment

Technology / **Published On October 29, 2019 11:50 PM /**

Ernice Gilbert October 29, 2019

The credit and debit cards of multiple Virgin Islands residents tied to their WAPA account were compromised recently, with two residents -- one whose card was charged $363 for soccer tickets in France, and another whose U.S. bank blocked multiple transaction attempts -- telling the Consortium of the occurrences Tuesday. The hackers attempted four transactions on the debit card tied to the local bank, but the customer's bank, Banco Popular, blocked three, the Consortium was told by one of the affected customers. This WAPA customer also told the Consortium that he was on his way to work and stopped to

put gas in his vehicle, only to be told that his Visa debit card declined.

The Consortium contacted Jean Greaux, WAPA director of communications Tuesday afternoon for comment. Mr. Greaux said he was not aware of any hack that had affected the third-party payments vendor that WAPA uses for the credit and debit card payment of bills.

But in a release issued Tuesday night, WAPA advised its customers who pay their electrical and water bills online to ensure that "no questionable or fraudulent charges have been made on their credit or debit card accounts."

WAPA revealed that the third-party vendor used by the authority to process credit and debit card payments was indeed the target of a cyberattack. The authority reminded residents of its other payment options as it continues to monitor the situation.

The payments system, named Click2Gov, was targeted by hackers who managed to compromise the system. The flaw was first discovered in December 2018 after continual breaches of it led to the compromise of at least 294,929 payment cards across the country, according to news reports.

WAPA said Tuesday that after a customer reported fraudulent activity on their credit card account following an online payment, the authority immediately, on October 18, notified its vendor, Central Square Technologies, parent company of Click2Gov, about the possibility of a data compromise.

Yet even though the authority said it knew of the breach since Oct. 18, it did not inform the public until the Consortium contacted Mr. Greaux today about multiple customers whose debit cards were compromised as a result of the Click2Gov hack. At least two of the accounts the Consortium is aware of were hacked on Sunday -- nine days after WAPA said it learned of the compromise.

WAPA said in its Tuesday release that Central Square Technologies, which the authority said has processed WAPA’s online payments for more than a decade without incident, has since taken steps to prevent reoccurrence.

The authority said it has a meeting with Central Square Technologies on Wednesday and will provide additional updates. The vendor is in the midst of an investigation on the scope, cause, and remediation of the data breach involving WAPA’s online payment methods, WAPA said.

Executive Director Lawrence J. Kupfer said Tuesday night that as a precaution, WAPA provisioned new servers to avoid reoccurrence. ”WAPA is working with Central Square Technologies to determine the number of customers affected, and the dates that the compromise occurred. Payments made by two other options, self-service kiosks, and pay-by-phone were not affected,” he said. Mr. Kupfer encouraged customers to monitor credit card statements for potentially fraudulent activity, according to WAPA. “Any suspicious charges should be reported to your bank or credit card provider immediately.

© Viconsortium 2026