The Virgin Islands Consortium

Credit and Debit Card Hack Through WAPA Appears to be Widespread in Virgin Islands; WAPA Says Support Services Will be Made Available to Affected Customers

Business / **Published On October 31, 2019 10:47 AM /**

Ernice Gilbert October 31, 2019

WAPA and its third-party payments vendor, Central Square Technologies, the parent company of Click2Gov, an online payments firm that was hacked, leading to the compromise of credit and debit cards of many Virgin Islanders, said support services would be provided to those affected by the hack, which appears to be widespread in the U.S. Virgin Islands.

Many Virgin Islanders have been reporting fraudulent activity, including some who called the Consortium directly to talk about what happened. One resident said she had been

back and forth with her bank for the past few days after a total $1,500 was fraudulently debited from her account through the same card tied to her WAPA account. "When I saw the story this morning I jumped out of my bed and suddenly realized what happened. This happened to me," this person told the Consortium Wednesday morning after reading our story.

Another resident contacted the Consortium through Facebook on Tuesday night and said $214 was fraudulently debited from their bank account through the debit card tied to WAPA. This happened on Tuesday, this person said. The two WAPA customers who initially contacted the Consortium about the fraudulent activity, said their accounts appeared to have been compromised on Sunday.

WAPA, however, said the hack of Click2Gov was fixed on Oct. 25, which was last Friday. Additionally, the authority in its latest release sought to explain why it didn't notify the public sooner after stating on Tuesday night that it learned of the possible compromise on Oct. 18, and notified Central Square Technologies about the breach the same day.

WAPA said in its Wednesday release that a customer made an initial report that her card had been compromised after making an online payment with WAPA. The authority said it then contacted Central Square to open an investigation. A forensics auditor determined that, at that time, the payment portal was not compromised, WAPA said. However, Click2Gov -- which was compromised in 2017 -- was again compromised in August 2019, two months before the latest WAPA breach.

WAPA said a second customer notified the authority on October 22 of a similar incident involving a credit card, and Central Square later confirmed the cyberattack and noted that the Click2Gov application was hit by a "never before seen attack."

Yet even after the Oct. 22 incident, WAPA did not issue an advisory. It was not until the Consortium contacted the authority about the hack on Oct. 29 that WAPA hurriedly issued a statement to notify its customers.

The authority added that Central Square on Oct. 25 developed and implemented a security fix.

"Since last week Friday, there have been no new reported instances of fraudulent credit card activity involving WAPA customers," WAPA said, a claim that goes against the complaints of customers, a number of whom reported incidents as recently as Oct. 29.

Statement from WAPA CEO Lawrence Kupfer

“We met today with representatives of Central Square who are carrying out an investigation on the scope and cause of the cyberattack. The effort continues to determine the date range of the cyberattack and the number of customers whose credit card information was compromised while their payment transaction to WAPA was being processed.

“In our discussion with Central Square today, WAPA was reassured that there have been no further compromise incidents since October 25, when the threat against WAPA’s customers was identified and security fixes were immediately implemented. These requirements are established by the major credit card companies to ensure the secure

transmission, storage and handling of cardholder information."

Are your credit and debit cards protected?

WAPA said it was told by Central Square that the only cards impacted were those being entered to the payment process in real time. WAPA further stated that it does not store customer information, but that's a non-factor since the information is stored by Click2Gov -- which was hacked.

The authority also tried to instill confidence in Central Square by calling it an industry leader in public administration software, serving over 7,500 organizations. "WAPA has been using Central Square for over 10 years without any previous incidents," the authority said.

But Central Square's Click2Gov has been compromised on a number of occasions, according to news reports, and “the portal remains a viable attack surface,” researchers have said.

Eight US cities were impacted by a breach in August, with six already having systems that were previously compromised in the original 2017 breach.

“These eight cities were in five states, but cardholders in all 50 states were affected,” researchers said. “Some of these victims resided in different states but remotely transacted with the Click2Gov portal in affected cities, potentially due to past travels or to owning property in those cities.”

Researchers contacted the eight towns, and while most did not respond, those that did confirmed a breach in their Click2Gov utility payment portals, according to a report from Threat Post, a news site that covers IT and business security for hundreds of thousands of professionals worldwide. Also, several towns took their Click2Gov portals offline shortly after contact. The breach was also reported by tech news site ArsTechnica.

Researchers said organizations must regularly monitor their systems for breaches and keep up to date on patches.

“The second wave of Click2Gov breaches indicates that despite patched systems, the portal remains vulnerable,” the researchers said. “It demonstrates cybercriminals’ willingness to repeatedly target the same victims and underscores that while responsible security habits are constructive, there is no perfectly secure system.”

© Viconsortium 2026