

Breaking & Exclusive!

EXERCISE EXERCISE EXERCISE

Acme Air Inc. Investigating Credit Card Breach by Cyber Criminals

Sources say that Acme Air Inc. has hired an outside investigative firm to look into a possible data breach, potentially involving millions of customer credit and debit card records, and possibly other information as well. The sources indicate that the criminals may have breached systems in November, ahead of Thanksgiving, in anticipation of the busiest travel timeframe of the year.

Multiple sources from top credit card issuers have confirmed that the breach has impacted nearly all Acme Air locations worldwide, and involves the theft of data stored on the magnetic stripe of cards used at the stores. Additionally, there are unconfirmed reports that Acme Air Inc.'s website has been hacked as well to siphon off additional credit card information (and possibly personal information, including logins) from unsuspecting passengers.

Initially investigators thought the breach may have encompassed just two weeks in May, but unconfirmed reports have pointed towards evidence the breach may have begun sometime just before March. The breach has affected an unknown number of Acme Air's customers who utilized the company's airport kiosks during that time. The investigation is still on going in regards to the online portal.

"The incident seems to continually be getting worse," said an investigator close to the breach. "At first it appeared to be fairly isolated, but as we've continued to peel back the layers of the proverbial onion, it seems to be a rather extensive breach. Most company locations have been impacted, as well as overseas. We're currently trying to determine if the online portals were affected as well."

Recently it was reported that millions of cards had been put up for sale on an underground forum known for selling stolen cards. While it is not verified these two incidents are linked, sources at major card issuers are beginning to see a pattern linking the two.

Looking to a previous incident- in 2013, retailer Target disclosed that thieves had broken into its central IT systems via a third party Heating, Ventilation and Air Conditioning partner, and used the access to install malicious software to its Point of Sale terminals allowing them to steal credit card track data on more than 40 million cards. It's still unclear what happened at Acme Air, Inc., but these breaches are becoming more commonplace with criminals leveraging the weakest points in networks to achieve their goals. Like previous breaches of this magnitude, there may be an impact in the hundreds of millions of dollars coupled with high-level resignations.

Acme Air, Inc. has not responded to multiple requests for comment.

Credit to Brian Krebs for inspiring this mock-up: <http://krebsonsecurity.com>

EXERCISE EXERCISE EXERCISE

From:

<https://bgp4all.com/pfs/> - **Philip Smith's Internet Development Site**

Permanent link:

https://bgp4all.com/pfs/training/itu-ipv6/ttx_script2

Last update: **2016/05/25 08:39**

