2-USA Today-US Postal Service hacked

U.S. Postal Service hacked, told Congress Oct. 22

Elizabeth Weise

USA TODAY

In classified briefings Oct. 22 and Nov. 7, the U.S. Postal Service told members of Congress that it had been hacked.

The service made the information public Monday.

The Washington Post reported China may have been involved in the cyberattack, citing anonymous sources. USA TODAY was unable to confirm the report.

Postal Service spokeswoman Sue Brennan told USA TODAY the “issue is still under investigation. *[Deny]*”

In its statement, the post office said some USPS computers were hacked and some employee information was compromised.

Information about people who called in to the post office’s Customer Care center was also compromised.

The service’s customer website, usps.com, was not affected, the statement said.

“The intrusion is limited in scope, and all operations of the Postal Service are functioning normally,” said David Partenheimer, media relations manager for the U.S. Postal Service. *[Diminish]*

In a letter sent Monday, Rep. Elijah Cummings, D-Md., cited the classified briefings, which were made to the House Committee on Oversight and Government Reform. He asked for more information from Postmaster General Patrick Donahoe.

Cummings asked for a description of the cyberattack and how it was first discovered, as well as what actions Donahoe took after learning about it.

The post office is investigating the incident. The investigation is being led by the FBI and other federal and postal investigatory agencies. *[Rebuild]*

Employee information that might have been compromised included personally identifiable information about employees, including names, dates of birth, Social Security numbers, addresses, beginning and end dates of employment, emergency contact information and other information.

Roughly 800,000 employees were affected by the intrusion, the service said.

If indeed China is behind the attack, it's likely part of an attempt to gain more information about U.S. government, said Edward Ferrara, an analyst with Forrester, a technology research company.

Employee data is also very helpful for future attacks.

"If a relatively high-level employee at the post office starts sending out phishing attacks from a .gov address, it's a possible stepping stone for attacks to get information of more value elsewhere," Ferrara said. *[Worry]*

Cash registers and point-of-sale terminals in post offices, as well as the website usps.com where customers pay for services with credit and debit cards, were not touched by the incident.

There is no evidence any customer credit card information from retail or online purchases such as Click-N-Ship, the Postal Store, PostalOne!, change of address or other services was compromised, the service said.

Also possibly affected were call center data for customers who contacted the service's Customer Care Center by telephone or e-mail between Jan. 1, 2014, and Aug. 16, 2014, Partenheimer said.

According to the Postal Service's website, the Customer Care Center handled 83 million inquiries in 2013.

The compromised data consist of names, addresses, telephone numbers, e-mail addresses and other information for customers who gave the information when they called or e-mailed in.

The service said that it does not believe potentially affected customers need to take any action as a result of the incident. *[Diminish]*

"We began communicating this morning with our employees about this incident, apologized to them for it, and have let them know that we will be providing them with credit monitoring services for one year at no charge to them," Partenheimer said. *[Rebuild]*