UNITED STATES POSTAL SERVICE®

U.S. POSTAL SERVICE BREACH: A TIMELINE

At a Nov. 19 congressional hearing, Randy Miskanic, vice president for secure digital solutions at the United States Postal Service, provided details about its data breach and how the Postal Service responded.

2.9 MILLION

Customers' names, addresses, phone numbers, e-mail addresses – **compromised.**

800,000

Employees' names, dates of birth, Social Security numbers, addresses, beginning and end dates of employment, emergency contacts – **compromised.**

SEPT 11 2014

Inspector General notifies the USPS about the breach. Days later, IG advises the USPS CISO that the investigation should remain confidential.

The IG, postal inspectors and members of the CISO team meet to develop steps to investigate incident.

SEP 16-19

U.S. POSTAL SERVICE SEP 19 to OCT 2

IG agents and postal inspectors configure and install technical architecture and tools to identify affected servers and workstations.

Investigators discover a large data file has been copied and removed from the USPS network. The file was encrypted, limiting the ability to identify the data it contained. Officials suspect that the file was copied to another server outside the USPS network controlled by an adversary.

OCT 7

U.S. POSTAL SERVICE OCT 11-15

After a forensic examination, IG investigators and postal inspectors surmise the pilfered data was contained in a Postal Service Human Resources file that included employee PII.

Recovered employee PII from the compromised server was reconstructed and shared with the USPS chief human resources officer.

OCT 26-28

U.S. POSTAL SERVICE OCT 31

Investigators identify a database backup file on a compromised server, which related to an application used for receiving, processing and managing customer service requests.

USPS confirms employee PII was copied and stolen from the Postal Service network.

NOV 4

NOV 7

The Postal Service CIO activates a remediation plan developed with U.S.-CERT guidance and supported by external cybersecurity experts.

Implementing elements of the remediation plan require a network brownout, which limited communications between the Postal Service network and the Internet.

NOV 8-9

U.S. POSTAL SERVICE NOV 10

USPS publicly acknowledges a "cybersecurity intrusion" into some of its information systems.

Continuing Action: USPS blocks employees' access to e-mail sites, such as Gmail and Yahoo, to reduce the likelihood of phishing and spear-phishing attacks.

View this infographic online
http://www.databreachtoday.com/us-postal-service-breach-timeline-a-7606

Source
U.S. Postal Service

Data Breach TODAY
Prevention. Response. Notification.