UNITED STATES POSTAL SERVICE ®

USPSNEWSBREAK

Nov. 10, 2014

Notification of cyber intrusion and employee data compromise

The Postal Service recently learned of a cyber intrusion into some of its information systems and an investigation began as soon as the intrusion was discovered. Steps already have been taken to strengthen the security of USPS systems and there will be additional measures in the coming days and weeks.

The investigation indicates that files containing employee information were compromised, including names, dates of birth, social security numbers, addresses, beginning and end dates of employment, and emergency contact information for all active employees. In addition, we are aware of a possible compromise of injury claim data that we are still investigating involving a small number of employees. Individualized letters will provide everyone with specific information about their particular situation.

PMG Patrick Donahoe has recorded a special video for employees with background information, an explanation of steps being taken to protect employees, and an explanation of resources available on the cyber incident.

“I’d like to say how bad I feel that the whole organization has been victimized,” says Donahoe. “The Postal Service has put in a lot of effort over the years to protect our computer systems and the bad guys haven’t been successful until now.”

Donahoe apologized that the incident happened. “You also have my commitment that we will help all of our employees deal with the situation,” he said. “We are a resilient organization and we’ll get through this.”

The video can be viewed from the postal intranet *Blue* on any postal computer, or from your personal computer on the Postal Service YouTube channel: *youtube.com/user/uspstv*.

A 1-page employee handout, which can be found on the next page of this *Newsbreak*, is being provided to all employees.

You also can check special pages being posted on the *Blue* (*blue.usps.gov*) and *LiteBlue* (*liteblue.usps.gov*) employee websites at 11:30 a.m. EST, Nov. 10. The *Blue* website is available from any postal computer on the postal internal network. *LiteBlue* is available from any computer connected to the Internet. You will need your Employee ID number and your employee password to access *LiteBlue.* Check the *Blue* or *LiteBlue* home pages for a new box titled: *“!! Important Employee Information !!”* in the left column.

Along with the handout, online resources include: an employee video, a stand-up talk and FAQs. Please check the handout and resources for more information.

In addition, the Employee Assistance Program is available for specific concerns you may have, at *EAP4YOU.com* online, or by phone at 800-327-4968; TTY 877-492-7341.

Please continue to the next page of this notification for the *Employee Handout*.

PLEASE PRINT AND POST ON ALL EMPLOYEE BULLETIN BOARDS.

UNITED STATES
POSTAL SERVICE

USPS Cyber Intrusion and Employee Data Compromise Employee Handout

This document provides you with information about the recent cyber incident. It is meant to accompany a stand-up talk from your manager/supervisor, after you've seen a special PMG video message, and/or stand-up talk on November 10, 2014. All impacted employees will receive a letter at their address of record within ten days.

Situation

The Postal Service recently learned of a cyber intrusion into some of our information systems. This basically means that someone who didn't have permission was able to get into some of our computer networks. This type of intrusion is not unique; you likely have read multiple news stories on similar intrusions into U.S. companies and other Federal government agencies.

We began investigating the intrusion into our systems as soon as we discovered it. We are working closely with the FBI, the Department of Justice, our own Inspector General and Postal Inspection Service, and the U.S. Computer Emergency Readiness Team. Additionally, we've brought on outside experts who specialize in investigations and data systems to help us understand what happened and how to improve our security.

What Information Was Compromised?

The investigation indicates that files containing employee information were compromised. These files include information such as names, dates of birth, social security numbers, addresses, beginning and end dates of employment, and emergency contact information for all active employees. It may also include the same information for any employee who left the organization anytime from May 2012 to the present. In addition, we are aware of a possible compromise of injury claim data that we are still investigating involving a small number of employees. We are unaware of any evidence that the compromised employee information has been used to engage in malicious activity.

What Should I do?

There are some steps you can take. A personalized letter from the Postmaster General is being sent to your home address via First-Class Mail with an enrollment code for a credit monitoring service that is being provided to you free of charge for one year. Please take advantage of this free service. If you do not receive your letter by November 20, please contact the Human Resources Shared Services Center (HRSSC) at 1-877-477-3273, and choose option 5 (option 1 for TDD/TTY), Monday through Friday, from 7 a.m.– 8:30 p.m., ET.

Please also visit Blue or Lite Blue for more information and FAQs about protecting against misuse of your personal data. If you need to speak with someone directly about your situation, please contact the HRSSC or you can also discuss this matter with your local human resources representative.

What Should I Say if Customers Ask About This?

The operations of the Postal Service are not impacted – Post Offices are functioning normally and mail and packages are being delivered as usual. While the investigation is ongoing, the compromised data relates to employees' information. The intrusion also compromised call center data submitted by customers who contacted the Postal Service customer care center with an inquiry via telephone or e-mail between January 1, 2014 and August 16, 2014. This data consists of names, addresses, telephone numbers, e-mail addresses and other information for those customers who may have provided this information.

PLEASE PRINT AND POST ON ALL EMPLOYEE BULLETIN BOARDS.