UNITED STATES
POSTAL SERVICE

USPS Cyber Intrusion and Employee Data Compromise
Updated Dec. 18, 2014
Frequently asked questions

1. **How and when did the security breach occur?**
The Postal Service recently learned of a cyber-security intrusion into some of its information systems. This intrusion was similar to attacks being reported by many other federal government entities and U.S. corporations. We are not aware of any evidence that any of the potentially compromised customer or employee information has been used to engage in any malicious activity.

2. **What customer data was compromised?**
Postal Service transactional revenue systems in Post Offices as well as on usps.com where customers pay for services with credit and debit cards have not been affected by this incident. There is no evidence that 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.

   Call center data submitted by customers who contacted the Postal Service Customer Care Center with an inquiry via telephone or e-mail between Jan. 1, 2014, and Aug. 16, 2014, was potentially compromised. For most of our customers in this group, the file did not include sensitive personally identifiable information. However, the ongoing investigation has revealed that the information potentially compromised in the incident included personally identifiable information that customers may have submitted to the Postal Service such as their name, address, telephone number, email address, and payment card number. To our knowledge, the data potentially accessed did not include Credit Verification Codes (CVC), Personal Identification Numbers (PIN), or any other payment card information. For those customers who provided their credit card numbers between Jan. 1 and Aug. 16, 2014, the Postal Service will offer the same one-year free credit monitoring product being offered to Postal Service employees and some retirees. This small group of customers (approximately 100) will receive a letter with additional details about the cyber breach and instructions on how to enroll in the free credit monitoring service. At this time, we do not believe that any other customers potentially affected by the incident need to take any action. We are unaware of any evidence that the compromised customer information has been used to engage in malicious activity or to enable identity theft crimes.

3. **Who is the Postal Service working with to investigate this cyber security intrusion?**
We are working closely with the Federal Bureau of Investigation, Department of Justice, the USPS Office of Inspector General, the Postal Inspection Service and the U.S. Computer Emergency Readiness Team. The Postal Service has also brought in private sector specialists in forensic investigation and data systems to assist with the investigation and remediation to ensure that we are approaching this event in a comprehensive way, understanding the full

implications of the cyber intrusion and putting in place safeguards designed to strengthen our systems.

4. **Why were customers not told of the cyber breach immediately after it was discovered?**
   Communicating the breach immediately would have put the remediation actions in jeopardy and might have resulted in the Postal Service having to take its information systems offline again. We are unaware of any evidence that any of the compromised information has been used to engage in any malicious activity.

5. **Were recent weekend information network system problems (11/8-11/9) connected to the breach incident?**
   Yes. The Postal Service took some systems off-line as part of the cyber security intrusion mitigation efforts. We know this caused an inconvenience to some customers but this was an important step to improve our systems and help prevent future sophisticated cyber incidents from occurring similar to those that have affected other major corporations and government agencies.

6. **Since employees are being offered free credit monitoring for one year, is the same service available for customers who contacted the Customer Care Center?**
   The comprehensive investigation has not resulted in any evidence that credit monitoring is needed for customers. Moreover, for both customers and employees, we are not aware of any evidence that any of the potentially compromised information has been used to engage in any malicious activity.

7. **How does the breach affect customers who take advantage of the Postal Service's partnership with companies like FedEx and UPS – such as "last mile" services?**
   The investigation has found no compromise of customer data from these services. The only customer impact found as a result of the investigation is some information provided by customers who contacted the Postal Service Customer Care Center with an inquiry by phone or e-mail between Jan. 1, 2014, and Aug. 16, 2014. This compromised data consists of names, addresses, telephone numbers, e-mail addresses and other information for those customers who may have provided this information.

8. **What is the impact of the breach to suppliers and contractors?**
   Based on the results of the investigation thus far, we are not aware of any implications for suppliers/contractors as a result of the cybersecurity intrusion.

9. **What precautions have been taken since the breach?**
   We are instituting numerous additional security measures, some of which are equipment and system upgrades that will not be visible to users, and some are changes in employee policies and procedures that we will be rolling out in the coming days and weeks.

10. **Have any lessons been learned from this?**
    The security of our information systems has always been a top priority of the Postal Service. Despite this, the Postal Service has now joined the growing list of major companies and governmental agencies that have been breached in similar ways. Customers can count on the Postal Service to safeguard personal information. This is a responsibility we continue to take very seriously. The entire leadership of the Postal Service is committed to taking steps to strengthen the security of its systems.

11. **Independent surveys show customers identify the Postal Service as a highly trusted government agency and company. Why should customers and employees continue to trust the Postal Service with their sensitive information?**
    The Postal Service has earned its reputation as one of the most trusted companies and government agencies in the country. The privacy and security of employee and customer data is of the utmost importance to us. Despite devoting a great deal of time and attention to the security of our information systems, the Postal Service joins the list of major companies and government agencies that have had similar cyber intrusions. The remediation efforts we took to address the cyber breach have resulted in an even stronger system to protect our data. The entire leadership of the Postal Service is committed to taking steps preventing something like this from happening again.

12. **I recently applied for and obtained a passport through the Postal Service. Is my personal information at risk due to this breach?**
    No. The investigation has resulted in no evidence of any customer data being compromised from the passport application process.

13. **I'm concerned about a *New York Times* article that mentioned "surveillance" of mail. Is this connected with the cyber-intrusion incident and what is meant by "mail covers"?**
    The *New York Times* article is unrelated to the cyber breach. The *Times* article titled "Report Reveals Wider Tracking of Mail in U.S." published on Tuesday, Oct. 28, 2014, is extremely disappointing. The article is inaccurate and unfairly presents a one-sided version of the facts. First and foremost, the United State Postal Service respects the privacy of its customers and the sanctity of the mail. Contrary to what is suggested in the article, the Postal Service does not monitor the mail behavior of its customers and it does not maintain any system or program of so-called "surveillance." Unfortunately, and perhaps to create a news story where there is none, the *New York Times* article conflates three independent mail programs in order to create the wholly false impression that there is some vast mail monitoring system in operation. While such an assertion may make for a more interesting news article – it is not based on the facts. Mail covers are used for criminal investigations. The increased use of mail covers in 2013 and 2014 is connected to single packages investigated involving illegal drug shipments. Eighty percent of all mail covers in 2014 were related to these important investigations. All other mail covers have actually decreased by more than 30 percent since 2012. It is unfortunate that the *New York Times* presented such a distorted view of the facts. Its readership would

have benefited from a more even-handed approach. The Postal Service processed and delivered 158 billion pieces of mail last year, of which only a tiny percentage was subjected to the mail cover process. The people who need to be concerned about mail covers are those who use the U.S. Mail to ship illegal drugs or who are otherwise breaking the law.