UNITED STATES POSTAL SERVICE

USPS Cyber Intrusion and Employee Data Compromise
November 10, 2014
Employee Frequently Asked Questions

1. **How and when did the security breach occur?**
   The Postal Serve recently learned of a cyber intrusion into some of its information systems. 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 are not aware of any evidence that any of the compromised employee information has been used to engage in any malicious activity. 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 insure that we are approaching this event in a comprehensive way, understanding the full implications of the intrusion and putting in place safeguards designed to strengthen our systems.

2. **Why were employees not told of the breach immediately after it was discovered?**
   Communicating the breach would have put the remediation actions in jeopardy. We are unaware of any evidence that any of the compromised employee information has been used to engage in any malicious activity or to enable identity theft crimes.

3. **Which Postal Service employees were impacted by the breach?**
   Files containing personally identifiable information (PII) for all active employees were compromised. Employees affected include the Postmaster General, other members of the Executive Leadership Team, PCES and EAS employees, craft employees and all other employees. It also includes employees who work for the Postal Inspection Service, the USPS Office of Inspector General and the Postal Regulatory Commission. These files may have also included PII for employees 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. Individualized letters will provide everyone with specific information about their particular situation.

4. **What information was accessed?**
   While the investigation is continuing, we have determined that the information potentially compromised in the incident included some employee personally identifiable information (PII) such as names, dates of birth, social security numbers, addresses, beginning and end dates of employment, emergency contact information and other information. In addition, we are aware of a possible compromise of injury claim data that we are still investigating involving a small number of employees.

5. **How could the Postal Service let all this employee information get accessed?**
   No company or organization connected to the Internet is immune from the type of malicious cyber activity the Postal Service experienced. We take such threats seriously and regularly take action to protect our networks, our customers' data, and our employees' information. In this case, a sophisticated actor was able to get around our defensive measures. As a result of this incident, we have significantly strengthened our systems against future cyber intrusions.

6. **Why were Postal Service information networks taken off-line before the breach was announced?**
   To improve the security of our information networks, the Postal Service performed maintenance and upgrades of its computer and information systems during the weekend of Nov. 8-9, 2014, bringing some systems off-line. This process allowed the organization to eliminate certain system vulnerabilities.

7. **What steps can I take to protect myself and avoid becoming a victim?**
   Because of the personal nature of the information involved, here are some steps you should take to protect yourself:
   - Enroll in Equifax Credit Monitoring – the Postal Service is making this product available to all employees at no charge for one year. You have 90 days from the date of a letter your will receive from the Postal Service to take advantage of these services, which are designed to help protect you. We encourage you to take advantage of this product. (Your unique activation code is at the top of the letter you will receive).
   - Keep vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. If you discover any suspicious or unusual activity on your accounts or you suspect fraud, be sure to report it immediately to your financial institutions and to local law enforcement. Additionally, the Federal Trade Commission provides comprehensive information at www.ftc.gov/idtheft, or call the FTC's identify theft clearing house at 1-877-438-4338 (TTY: 1-866-653-4261), or write to Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
   - On an ongoing basis, you should obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf . You can also purchase a copy of your credit report by contacting one of the three national credit reporting agencies. You may contact the national credit reporting agencies at:

- Equifax: 1-800-525-6285; or www.equifax.com; or P.O. Box 740241, Atlanta, GA 30374-0241.
- Experian: 1-888-397-3742; or www.experian.com; P.O. Box 9532, Allen, TX 75013-9532
- TransUnion: 1-800-680-7289; or www.transunion.com; P.O. Box 6790, Fullerton, CA 92834-6790

8. **What if I want to continue to receive credit monitoring from Equifax beyond one year? Can I renew by enrollment or will I have to start the process all over?**
   Equifax will notify employees prior to the end of their free subscription period that their subscription will be expiring. Employees will be given an opportunity to extend the subscription at their expense.

9. **Should I change my ACE ID and password, Postal EIN or other postal passwords as a result of this incident?**
   At this time there is no requirement to change your ACE password or other passwords unless prompted to do so by email prompts from IT as part of the normal password change process. You will be notified if other password changes are required. Your Postal EIN and ACE ID will not be changing as a result of this incident.

10. **How do I know if my banking information was affected by this breach? Should I call my bank and creditors?**
    We are unaware of any evidence that the compromised employee information has been used to engage in malicious activity. Postal Service forensic investigators are conducting a thorough review of the affected databases and if the ongoing investigation determines that any additional employee information has been compromised, you will be notified. Postal employees, like everyone else, should keep vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or you suspect fraud, be sure to report it immediately to your financial institutions and to local law enforcement. Postal employees, like anyone else, can always contact their bank or other financial institutions to change their account information if they wish to do so.

11. **What precautions have been taken since the breach?**
    Through the investigation we identified the methods and locations that were used to gain access to some of our data systems and devised a plan to close those access routes to our infrastructure to prevent future intrusions. Additionally, we are instituting numerous additional security measures, some of which are equipment and system upgrades that will not be visible to any users, and some of which are changes in policies and procedures that we will be rolling out in the coming days and weeks.

12. **Why is VPN not working? When will it come back and will there be any changes to it?**
    VPN was identified as vulnerable to this type of intrusion and will remain unavailable as we work to make modifications to this type of remote access to our networks. When VPN is available again users will notice changes in functionality. We will have additional information about VPN in the near future.

13. **Will I be held liable for ANY fraudulent activities on my personal information or banking accounts?**
    By enrolling in the free Equifax Credit Monitoring product, you will receive up to $1 million in identity theft insurance with no deductible and no other cost to you. Again, we are unaware of any evidence that the compromised employee information has been used to engage in malicious activity or to enable identity theft crimes.

14. **Have any lessons been learned from this?**
    The security of our information systems has always been a top priority of the Postal Service. Now the Postal Service has joined the growing list of major companies and governmental agencies that have fallen victim to cyber intrusions. Despite this breach,we will continue to make every effot to safeguard employee's 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 our systems and provide you with the resources you need as a result of this incident.

15. **I wish to speak to someone about these issues. Who should I contact?**
    Please contact the Postal Service Human Resources Shared Services Center at 1-877-477-3273 and chose option 5 (option 1 for TDD/TTY). You can also discuss this matter with your local human resources representative.

16. **Are the services of the Employee Assistance Program available in connection with this incident?**
    The Postal Service Employee Assistance Program is available to help any employee deal with this issue. Information or assistance is available 24 hours a day, 7 days a week. Please call 1-800-EAP-4-YOU (1-800-327-4968) or visit www.eap4you.com.