Employee video:

Today, I've got some tough news to deliver.

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 security intrusion isn't unique. You've probably heard about recent cyber intrusions into U.S. companies and several Federal Government agencies.

We began investigating the intrusion into our systems as soon as we discovered it.

We are now working closely with all the agencies you'd expect – the FBI, the Department of Justice, the Inspector General, our 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.

Because of the ongoing investigation – and the fact that letting anyone know about it could have kept us from fixing the problem – I couldn't tell you anything about this until now.

Here's what we've found: a file containing employee information was compromised. That file includes names, dates of birth, social security numbers, addresses, dates of employment, and emergency contact information for all active employees. It may also include the same information for employees who left the organization anytime after May 2012.

And we have seen no evidence that this information has been used for malicious activity, or for identity theft.

This incident impacts every employee in the organization – including me.

When we say that the information is compromised, it means that we can't be sure that there was data actually stolen from our network, but we cannot rule it out.

That's why we're taking some cautionary steps for every employee. Every employee is being offered a comprehensive credit monitoring product which the Postal Service will pay for. Every employee will receive a personalized letter at their home address in the coming week with directions about how to enroll in the free credit monitoring product.

We're also going to provide other assistance.

Today you'll receive some materials and hear from your managers about this incident. We're making the employee shared services line available to help with any specific questions or concerns you may have.

We're also providing resources on Blue and Lite Blue about this incident and offering suggestions for protecting against identity theft crimes.

So, where do we go from here regarding this incident?

We've already implemented some important security measures – that was the reason our network was off over the weekend. We will also roll out other new security measures in the coming days and weeks -- some of which are changes in policies and procedures – so stay tuned for that.

If you are asked by customers about this situation, you can tell them that it appears that no customer credit card or financial data was compromised. Our networks are functioning, mail and packages are being delivered, and it is business as usual for nearly every aspect of our operations.

On a personal note, I'd like to say how bad I feel that the whole organization has been victimized. The Postal Service has put in a lot effort over the years to protect our computer systems and the bad guys haven't been successful until now.

You have my sincerest apology that this has happened. You also have my commitment that we will help all of our employees to deal with this situation.

We are a resilient organization and we'll get through this.

Thank you very much for your attention and for the great work you do every day.

###