August 3, 2015

Dear Valued FedEx Customer:

The security landscape as we know it today is changing. As technology continually evolves, it is critical to stay ahead of those who wish to breach data security measures for their malicious benefit. It is important to understand that hackers do not select their targets based on the size of the organization, nor are data breaches unique to any one industry. FedEx continues to diligently work to ensure that all automation transaction technology and communication protocols are secure and up to date by proactively enabling, promoting and elevating strong encryption standards. This is achieved through several measures:

- Supporting the most up-to-date cryptographic technology
- Supporting the most up-to-date communications protocol
- Maintaining support for updated Microsoft operating systems, providing the most effective options for secure data transmission

Why this is important

Over the next year, FedEx will be updating its systems and technology allowing us to continue providing our customers the highest defenses possible. Planned initiatives include but are not limited to:

- **Retirement of SHA-1 technology**. The initiative to migrate from SHA-1 to SHA 256 (SHA-2) is the next proactive phase to better secure websites, intranet communications and applications. This migration will impact customers currently using Windows XP or Windows Server 2003. There will be a targeted communication regarding this migration effort dispersed to impacted customers during summer 2015.
- **Retirement of Windows XP and Windows Server 2003 support**. The 2015 market releases of FedEx Ship Manager® (FSM 290x), FedEx® Integration Assistant (FXIA 290x), and FedEx Ship Manager® Server (FSMS 15.0.1) will be the last versions to support Windows XP and Windows Server 2003 operating systems. There will be a communication regarding this retirement effort dispersed to impacted customers during fall 2015.
- **Retirement of Secure Sockets Layer (SSL) technology**. SSL has been in the market for over 20 years and no longer meets minimum security industry standards, due to security vulnerabilities in the protocol for which there are no fixes. It is critically important that entities upgrade to a secure alternative and disable any fallback to SSL. FedEx has already begun taking actions to eliminate this vulnerability. Required customer action will be assessed and communicated in January 2016.

Data is an organization's most critical asset. Our desire is to help our customers protect this asset. More information will be provided in the coming months regarding action to be taken to align with these security measures.

Please ensure that the appropriate team members are aware of this important update. Thank you for your time and attention. We appreciate your business.

The FedEx Automation Team