OFFICE OF CYBERSECURITY
& CRITICAL INFRASTRUCTURE PROTECTION
DEPARTMENT OF THE TREASURY

OCCIP

TLP: AMBER[1]

November 2, 2021

Sector Partners,

The Treasury Department has learned about abnormal behavior observed in certain point-of-sale devices manufactured by PAX Technology that indicates possible risks to customer data confidentiality. Treasury partners have conducted laboratory testing that indicated the examined PAX point-of-sale devices transmitted encrypted data to unknown third parties that appeared to be superfluous to normal payment transaction processing. Specifically, the superfluous transmissions were made in addition to transmissions required to process payments; were larger in size, count, and frequency than payment transactions; and were sent to domains in China not listed in the documentation provided by PAX Technology.

At this time, the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) assesses that this behavior presents risk to customer data confidentiality. OCCIP assesses the loss of such data as presenting a low severity threat to the U.S. financial sector. OCCIP does not believe that these devices present unique risks to data integrity or service availability.

At present, OCCIP does not believe that the use of PAX Technology devices poses unique risks to network security. PAX Technology maintains remote access to their point-of-sale devices, which is common within the retail payments industry as providers typically use this access to perform device maintenance. OCCIP is not aware of any attempt by PAX Technology to use their devices for disruptive or destructive purposes.

OCCIP encourages stakeholders in the U.S. financial system to adopt a risk-based approach to protecting the confidentiality of their customers' data, the integrity of their networks, and the availability of their services. Banks and financial service providers should apply this risk-based approach to their supply chains.

To report an incident or submit a request for information, please contact OCCIP at OCCIP-Coord@treasury.gov or by calling 202-622-3000.

Thank you,

Office of Cybersecurity and Critical Infrastructure Protection
U.S. Department of the Treasury

[1] TLP: AMBER sharing restrictions: Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.