Statement Regarding USA Technologies Data Security

The USA Technologies ePort, Seed Cashless and ePort Connect Service are designed to facilitate cashless payments (i.e. credit or debit card) primarily for the unattended, small-ticket point of sale industries, such as vending operations. The ePort and Seed Cashless will communicate wirelessly through the cellular network. All data transmission into and out of the ePort and Seed Cashless is strongly encrypted. The encryption keys are periodically changed to ensure adherence to the highest industry standards for secure communication. These devices only support communication that they initiate. Hence, there is no possibility of logging into either device or otherwise establishing direct communication with it. Only responses from the USA Technologies network are accepted by the ePort or Seed Cashless after the device first establishes an initial communication session with the USA Technologies network.

The ePort and Seed Cashless only read the card Track 2 data and retain that data in volatile memory only long enough to perform a card authorization. The track data is released from memory once the authorization response is received and is NEVER stored in the device for any reason. The primary account number (PAN) and expiration date are the only two pieces of data captured from the card by USA Technologies. No other data, such as the card holder's name, is captured. All data processing and storage occurs in the USA Technologies PCI compliant network. The ePort G-9 has been audited and determined to be out of scope for a PA-DSS v3.1 listing. This device and Seed Cashless fall under our PCI-DSS Service Provider PCI-DSS v3.2 certification as a secure network end-point. A security White Paper on the ePort G-9 is available upon request for more detail.

USA Technologies also offers a software interface to our systems using either the ePort SDK or ePort Quick Connect API. The use of these products requires that a compatible secure encrypted reader be used in order to ensure credit card data security is maintained end-to end. As the Third Party Payment Processor, USA Technologies assumes the risk for any credit card data breach from these systems. The USA Technologies business model was developed to ensure that our customers are effectively out in scope for PCI-DSS. If there were ever a data breach, USA Technologies would be responsible for managing all communication with our customers, card processors and the authorities.

In summary, no credit card data is ever stored in an ePort or Seed Cashless device and all communication is strongly encrypted. All communication is initiated by these devices and only to the USA Technologies network. USA Technologies maintains compliance as a PCI-DSS v3.2 Level 1 Service Provider and is currently listed on the VISA website at: http://www.visa.com/cisp . Annual PCI audits are performed to maintain this compliance level and to ensure the continued secure processing of credit card data.

USA Technologies, Inc. is responsible for the security of the card holder data. As such, we continually maintain all applicable PCI-DSS standards associated with our credit card processing environment.

Arthur M. Royce
Sr. Director of Security and Compliance

8/1/2018
Date

CISP Compliant