A GUIDE TO SECURITY AND COMPLIANCE

FOR AVANTI MARKETS' OPERATORS

 Version 1.3; Jan 2017

OVERVIEW

Avanti Markets strives to provide our operators with an understanding of the measures taken to protect sensitive data involved with payment card transactions. We understand the need for controls that foster the security and privacy of data at multiple layers of the data lifecycle, as well as the need to communicate an understanding of those controls to establish trust in our systems and services.

This document will be updated as Avanti Markets continue to make improvements to both our security and privacy controls, and in our communications of those controls to you.

PROTECTION OF DATA IN TRANSIT

Card transactions communicate directly with our partner bank systems. These transactions are protected by encryption capabilities that align with recognized industry standards, as well as encryption and communication requirements established by our card processing partners.

In addition, only defined and approved communications can converse with our backend infrastructure and support systems located within PCI compliant hosted Azure services. Monthly vulnerability scans are also run against key externally facing systems to identify communications and other types of threats and risks. Output from these as well as other periodic testing activities then feed into internal mitigation and risk strategies.

Since these communications are a part of kiosk and application functionality they fall outside the direct control of the location network owners. Therefore, kiosk communications between card processing services and Avanti Markets backend systems should be considered outside the scope of responsibilities for location network owners.

PROTECTION OF DATA AT REST

Upon transaction authorization only allowed card data as defined and permitted by PCI DSS standards is retained. All sensitive card data, including primary account numbers (PANs) are restricted to allowed formats, such as truncation and/or tokenization and align with defined PCI standards. All card data is also protected by additional measures such as segmentation, access controls, and encrypted databases as defined by PCI and industry standards.

In cases where a kiosk may go offline, due to a downed network for example, card data may be temporarily stored within our proprietary systems until the kiosk is online and in communications with the banks. During that time, all data is secured in an encrypted format aligning with PCI and industry requirements and standards. Upon successful authorization, sensitive data is securely removed and only data allowed by PCI standards is retained.

Hardening measures such as application testing and review are also leveraged to help ensure the secure functionality and operation of the integrated systems.

Backend infrastructure systems are segmented from kiosk operations, and deployed within PCI compliant hosted Azure environments. Physical access controls are employed and maintained by the hosted center operations in accordance with PCI requirements. Backend systems also undergo frequent vulnerability assessments such as ASV scans to help identify new and emerging threats.

DEVELOPMENT PRACTICES

Avanti employs software development best practices, utilizing industry standard software development tools and management environments. Multiple controls and processes such as code testing and peer reviews feed into our software development and change management programs. These controls and processes are integrated throughout multiple stages of our development lifecycles. Bug tracking tools and triage operations help identify, escalate, and track high priority issues to resolution. Separate development and production environments, as well as secured code repositories help ensure that only approved and authorized code is deployed to production operations.

The protection of sensitive data, including payment card data, is a primary focus of our development and operations teams. This is particularly critical as we work with our partners to re-assess our processes, adapt to ever evolving security needs, in addition to ensuring continued alignment to changes in our PCI reporting status to Level 1.

Avanti does not divulge the specific details of internal code testing and review practices but will be happy to share our Attestation of Compliance (AOC) report required by the PCI council, once we have successfully completed the full assessment and review of our internal practices.

PHYSICAL PROTECTION OF KIOSKS

Kiosk systems are locked with keys deployed to authorized users. All data retained within kiosk databases is encrypted and secured by a layered security approach. Physical access to the kiosk components does not allow access to encrypted stored data.

All kiosks are shipped and deployed in a secure physical state. However, since the deployment is not within Avanti controlled physical environments, Avanti works with operators to maintain the physical security of the kiosk devices. The kiosks undergo continual transaction, user access, and system monitoring.

The distribution of keys to kiosk locks is documented, and keys must be physically secured and accounted for at all times.

KIOSK REMOTE ACCESS

Remote access to kiosk systems for administrative purposes is controlled via secured and PCI compliant communications. Access is restricted to authorized users, leverages dual factor authorization, and limited to authorized communications channels and mechanisms.

INTERNAL PROCESSES

Additional controls are in place to secure internal systems, processes, and data. Industry best practices regarding security and compliance are considered at multiple stages and layers within our operations. Some of these include but are not limited to perimeter control, system configuration and hardening, business continuity, access control, vulnerability and risk management, as well as various types of administrative controls.

Avanti does not divulge the specific details of internal processes and practices but will be happy to share the Attestation of Compliance (AOC) report required by the PCI council, once we have successfully completed the full assessment and review of our internal practices.

IN SUMMARY

Information and communications regarding security and privacy controls, as well as compliance status will be communicated as our plans, initiatives, and messaging progress, but please feel free to contact the Avanti Markets team at support@avantimarkets.com to answer any questions you may have. For now, these are the main things you should know:

- Avanti Markets Inc. is the Master Merchant of Record for our Operators.
- Data protection does not end at the perimeter, but is implemented at multiple layers within our systems, and supporting services.
- Data protection does not just involve technology, but also involves our people and processes that interface with the data and systems.
- Our approach to data protection is under continuous review and development to meet ever evolving threats and risks, as well as changing industry standards and compliance requirements.

Thank you from the
Avanti Team!