
USA TECHNOLOGIES

Security Guidelines for Your Vending Operation

#V VXUD9871136 REV C



This document contains information that will help you protect your operation from fraud.

Please read thoroughly.

Introduction

At USA Technologies, Inc. we constantly assess and adjust our security posture with respect to credit card security. Maintaining the security of cardholder data and the confidence of our customers is our top priority. Following, please find a few security guidelines that we believe will have little impact on your business operations but will have the potential to greatly improve your security posture and better protect consumers from fraud.

As you may be aware, the last few years have been peppered with both credit card and personal data breaches globally. What you may not know is that almost all of the breaches could have been prevented by a few simple, precautionary measures by the operators. USA Technologies, Inc. continues to lead the unattended self service industry in credit card data security and is committed to ensuring that all processing executed through our trademarked Seed and ePort Connect system maintains the highest level of security possible for both operators and their consumers. As a merchant, there are some simple preventative measures that will ensure better consumer security and address any concerns individuals might have about using the credit card technology on your machines, making your operation even more secure.

The additional measures are easy to apply and can be completed in moments as your team is performing regular maintenance on the equipment. The goal is simply to be aware of the card acceptance device environment and be able to identify if any form of device tampering has taken place. By doing this, your team will dramatically improve your operation's credit card security.

Observing Your Card Acceptance Devices

The USA Technologies, Inc. engineering team and our third-party manufacturers work very hard at making our patented Seed and ePort hardware extremely difficult to compromise. That being said, one of the most effective methods to thwart device tampering is simple: observation. Ask yourself: Is the device in the same condition as it was the last time it was visited? (Most tampering can be observed with a keen eye or by simple hand manipulation of the surrounding environment.) A quick observation and manual check to ensure the equipment is securely in place each time you visit may be all that is needed.

Skimmers

Skimmers are found primarily on ATM machines (Figure 1) but in theory, similar technology could be applied anywhere (Figure 2). Skimmers are typically "covers" that go over or in front of an existing card slot. Some may even appear to extend to the card device. Each one has a small magnetic head and some simple electronics to capture credit card data and send it to a nearby person (or store the data for retrieval).

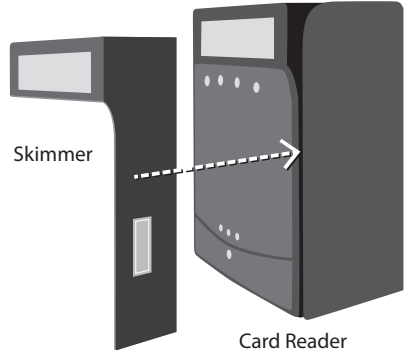
Evidence of tampering includes: traces of glue around the device, poor fit and noticeable gaps, and mismatched colors of the skimmer and the cardreader.

Internal Devices

FIGURE 1 – Example of an ATM Skimmer



FIGURE 2 – Possible Card Reader Skimmer



If there is no external evidence of tampering, a quick spot check can be performed each time the machine is opened for servicing or if it is ever found unlocked. Carefully review the card device installation AND wiring, a data acquisition and storage device can be very small, but extra wires connected to either the card reader or telemeter will guide you to any malicious equipment.

Shipping Locations

Remember, all new or used Seed and ePorts should **ONLY** be shipped to and shipped from:

USA Technologies, Inc.
3103 Phoenixville Pike
Malvern, PA 19355

Inovar, Inc.
750 East 1600 North
Logan, UT 84341

Conclusion

With a limited amount of effort in the field, it is possible for your team to ensure a safe environment for your customer's credit card info and ensure that your equipment maintains its secure state.

If you have any questions or concerns regarding this information please contact the USA Technologies Customer Care team anytime.



**100 Deerfield Lane, Suite 300
Malvern, PA 19355**

USA TECHNOLOGIES CUSTOMER CARE

Contact USA Technologies Customer Care for technical support and to request additional parts, information, and pre-authorization forms.

Phone: 888.561.4748

FAX: 610.989.9695

Email: customersupport@usatech.com

Online Store: <http://store.usatech.com>

USA TECHNOLOGIES WEBSITE ADDRESSES

Customer Website Login

<https://usalive.usatech.com>

Company Site

<http://www.usatech.com>

<https://www.cantaloupesys.com>

#VVXUD9871136 REV C

**All contents © Copyright 2018 USA Technologies, Inc.
All rights reserved.**