Compromised PIN-Entry Device Listing

Last Updated: December 06, 2013

Devices listed have been confirmed compromised and have been used in tampering and skimming attacks to capture PIN and magnetic-stripe card data*. All Visa clients must take action to mitigate the risks introduced by these compromised POS PEDs. Specific steps are outlined in *What to Do IF Compromised* guide that will help minimize the impact to your organization.

Vendor	Model	Lab Evaluation Status	Visa Requirement
Hypercom	S7S and S8	Devices never lab evaluated by Visa or PCI	Mandatory sunset date of 1 July 2010
Ingenico	eN-Crypt 2100	Pre-PCI Approved	Mandatory sunset date of 31 December 2014
Ingenico	eN-Crypt 2400 (also known as the C2000 Protégé)	Devices never lab evaluated by Visa or PCI	Mandatory sunset date of 1 July 2010
Ingenico	i3070EP01	PCI PED or EPP PED V1.X. Revoked PTS approval	Remove from production environments
Ingenico	i3070MP01	PCI PED or EPP PED V1.X. Revoked PTS approval	Remove from production environments
VeriFone Everest Plus	P003-400-01, P003-400-02 and P003-400-03	Devices never lab evaluated by Visa or PCI support only single Data Encryption Standard (DES)	Mandatory sunset date of 1 July 2010
VeriFone Everest Plus	P003-400-12 and P003-400-013	Pre-PCI Approved	Mandatory sunset date of 31 December 2014
VeriFone	PINpad 101, 201 and 2000	Devices never lab evaluated by Visa or PCI	Mandatory sunset date of 1 July 2010
VeriFone	SC5000	Pre-PCI Approved	Mandatory sunset date of 31 December 2014

**Clients may be liable and may be fined, if merchants are found using these devices past the mandatory Visa sunset date*