



**Mustang MicroSystems, Inc.**  
104 South Street  
Hopkinton, MA 01748  
P: 774•759•9000 F: 774•759•9035  
[www.mustang2000.com](http://www.mustang2000.com)

## Secure Disposal of Debit Payment Terminals and Encryption Keys

June 3, 2008

### Background

Debit payment terminals (also called Pin Entry Devices, or “PEDs”) collect consumer PINs as part of the debit card payment process, and they must be loaded with secret encryption keys to protect those PINs. Considerable effort has been taken to create and load the encryption keys, and they must be protected from the instant they are loaded into the terminals until the terminal is removed from service.

If the encryption keys in PEDs can be accessed, they can be used to gain access to consumer PINs. When a consumer PIN is lost and the account number is known the consumer’s cash can be immediately stolen using ATMs. There are several references to the issue of key protection in debit terminals in the Visa PIN Security Document (“*Visa Public Document 40026-02*”). In Objective 7 of security audit questions, there are two specific references:

Para 30: “Procedures exist that ensure the destruction of all cryptographic keys....within any cryptographic devices removed from service”

Para 32: “Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN processing equipment (e.g., PEDS and HSMS) placed into service, initialized, deployed, used, and decommissioned.”

Other references to PIN and key security in retail terminals can be found in the documents provided by PCI and by the X9 Standards organization, specifically in X9 Standard X9.24 Part 1. (*Retail Financial Services Symmetric Key Management*) [See [www.X9.org](http://www.X9.org)]

When retailer's POS systems reach end-of-life, it is normal to use a recycling service to responsibly dispose of equipment for recycling. Most retailers may not be aware that the debit terminals contain secret keys, and that the keys are critical to the retailer’s security until the keys are removed or the key is no longer used in any terminal within the retailer’s operating business.

Unless the recycler is trained and in compliance with the procedures, he cannot demonstrate that he is operating within published security standards.

### Specific Methods for PED Destruction of Key Removal

Proper removal of a PED debit key can be done by total destruction of the device, by crushing or by physical destruction of the secure PED elements. It has been shown that the old practice of opening the terminal case to disconnect power to the security chips and therefore “lose” the data is not sufficient, because the power does not drain away quickly enough to assure the keys have been lost.

For volume operations, there are large shredding machines that can destroy complete PCs, disc drives, and other electronics by grinding them into pieces not less than 5mm in size. These devices are applied in many areas where large amounts of sensitive data must be destroyed, as in the healthcare industry. Another method is to drill a large hole through the IC chips where the cryptographic keys and logic is located.

If the terminal boards that contain the security logic are ever intended to be re-used as spare parts, the keys must be removed by writing over the secret key with another debit key which is in itself secret. This is the process used at Mustang and by many other debit key service centers.

### Recommendation

Retailers or those who trade in new or used PEDs must be aware of these requirements so a retailer’s secret keys are not exposed. Mustang offers a secure key removal service, and our process also includes written certification (by serial number) that your terminals have been properly controlled and destroyed.

For information, please contact our sales department at the address above.