TO ALL KEY MANAGEMENT PERSONNEL:

THE COMPROMISE OF INTERCHANGE PINS AT NON-FINANCIAL INSTITUTION BRANDED ATMS HAS SUBJECTED THE VISA PAYMENT SYSTEM TO A HEIGHTENED LEVEL OF RISK. IN ORDER TO STAY IN COMPLIANCE, DATASTREAM / ASAI IS REQUIRED TO RECEIVE A SIGNED AGREEMENT FROM ALL ISOS REGARDING PIN PROCEDURES. PLEASE READ THE ENCLOSED INFORMATION CAREFULLY AND HAVE BOTH KEY ADMINISTRATORS SIGN THE DOCUMENT AND RETURN TO DATASTREAM / ASAI. YOUR PROMPT COOPERATION IS GREATLY APPRECIATED TO AVOID ANY FINES/PENALTIES.

PIN INJECTION AND KEY MANAGEMENT
Procedures and Forms

General Procedures

1. The objective of PIN and Key management security is to verify measures are documented and implemented to prevent any disclosure of clear text keys or their corresponding components.

2. Key components are maintained under dual control and split knowledge at all times.

3. Key parts are only combined in the secure key loading device and are not used for any other encryption process.

4. Key components used for one processor are not used for encryption for any other processor.
5. Do not inject any key component or encrypted keys into devices if there is any apparent damage or tampering with the device.

6. The processor is informed as soon as possible of any suspected key compromise.

7. Keys must be changed if there is any compromised key, suspected or known.

8. Keys that have already been encrypted under a device that is suspected of compromise must be recovered and reprogrammed.

9. A log is maintained of the times that key components are loaded into the PC key loading device.

10. The key administrators must make every reasonable effort to protect that component.

11. The procedure documents the current and past key administrators. If a key administrator leaves the firm and then returns he/she is only used as a key administrator for the same part as previously assigned. To prevent any possible coercion, two key administrators cannot directly report to the third administrator.

12. Keys will not be maintained in clear text form unless securely stored in a tamper resistant storage module (TRSM).

13. ISO Sales reps will be trained to instruct merchants to not request or accept a client's PIN in the event that a client asks for assistance in entering their PIN into the PIN pad.

14. ISO Sales reps will be trained to instruct merchants to make every possible effort to be sure that the entry of PIN's into PIN pads cannot be easily observed by others.

Receiving Key Parts

1. Their respective administrators receive Key parts A, B, and C. The key parts are received from the processor in separate tamper evident packages.

2. Upon receipt the key administrator inspects the envelope for tampering. In the event of tampering General Procedure #6 is activated.

3. Only the person entrusted as the key component holder (or backup holder) is authorized to open the document and this person must ensure that no other person can observe the printed key component.

4. The key administrator will inspect their respective key part to be sure that it is a double length key and that it appears to be a random key. If it does not appear to be random the security administrator will be alerted.

5. The key administrator brings the key part to the secure safe and stores the key in a marked lock box that is stored in the safe. One lock box for each key part is maintained and only the key administrator has a key to his respective lock box.

6. Two safes are used with two devices with split access.

7. The safe is stored in a limited access and locked non-working hours and within ops center that is locked. Limited access to room.

8. A Security Safe activity log is maintained and records each time the safe is opened as well as the date, purpose of safe opening, and parties involved in opening the safe.

Loading Key Parts

1. Key Administrators must enter the injection facility using the rules of split knowledge and dual control.

2. Although the PC is not a TRSM, compensating controls are applied to secure any device. The PC key injection device is inspected for tampering. Carefully inspect casing of equipment and interface cables associated with injection. The PC used does not have a modem or a network card installed. The PC uses a removable hard drive which is stored in the safe and only removed for PIN injection. (N/A at this time)

3. The key injection device software is started up and the key administrators load their respective passwords and key parts privately.

4. The key administrators then returns the key parts to the secure storage and the safe is closed and locked and the log entry confirmed. The security administrator verifies that the safe is securely locked and that the logbook has been updated.

5. The injector must inspect each ATM and POS device for tampering. Inspect POS devices for any signs out of the ordinary. Check the seams where the case connects together. Ensure no prying or modification of the device is detected.

6. The PIN pad is connected to the loading device and the PIN Encryption Key (PEK) is loaded into the device. This is repeated until all PIN pads scheduled for key injections are completed.

7. Upon completion of the PIN pad loading the PC is powered down. The shutdown is performed by the injection operator and witnessed by a 2nd key administrator.

8. The key entry log is updated to reflect the activity and record the PIN pad serial number and date of key entry.

9. Onsite installation of the keys is done via a vendor agreed supplier of ATM services. Both dual control and split knowledge concepts are used to protect key transport and life cycle process.

10. The following compensating controls are implemented:

11. A vendor is under the same privacy and data protection policies as an employee.

12. A TRSM is used to transport keys to the appropriate ATM site via Carrier such as FED EX and individually assigned key holders by names and prearranged agreement using dual control and split knowledge of key parts.

13. Each predetermined key holder receives their respective parts and checks for non- tampering packaging. Each key holder confirms receipt of the key part.

14. The key part is injected where no other can see key entry and the room is again inspected for compromise prior to key entry into an ATM.

15. The key part has been tracked and a key destruction form is enclosed for dual signatures and written documentation confirming the key part in clear text form has been destroyed beyond serviceability. No back up copy exist in the ATM locations.

Inventory Management

1. The loaded PIN pads are logged into inventory and stored securely until shipment to the merchant. No ATMs are preloaded.

2. The injected devices are stored in the locked, limited access injection room. A cabinet will be used to store inventory. Key administrator A and Key administrator B each possess one of the cabinet lock keys and maintain dual control over the cabinet.

3. Any devices returned for repair or for retirement have their injected PIN encryption key removed.

Key Component Destruction

1. Upon suspected compromise or in the event that new key parts are issued, the old key parts are to be destroyed.

2. Obtain request for key destruction. Requests must come from the security administrator or higher authority. The security administrator receives permission from Global to destroy the key parts.

3. The key administrators will obtain their respective key parts from the secure storage and destroy the key by burning in the kitchen sink.

4. The other key administrators view destruction and the key destruction form is completed to reflect the activity and then stored in the safe.

Key Compromise Procedures

1. If an Encryption Key of any type is known to be compromised the key must be immediately replaced with a new key.

2. Any organization that shares a compromised key should be contacted immediately and be made aware of the compromise.

3. New key components should be obtained from the processor.

4. Compromised Encryption Key components should be destroyed following Key Component Destruction procedures.

5. All above procedures should be completed within a maximum of 48 hours. This time frame includes transportation of key components.

SECURITY SAFE ACCESS ACTIVITY LOG

DATE	REASON FOR ACCESS	KEY ADMINISTRATOR 1 INITIALS	KEY ADMINISTRATOR 2 INITIALS

I HAVE READ AND AGREE TO ALL PIN INJECTION AND KEY MANAGEMENT PROCEDURES AND FORMS.

_____

ISO

_____

DATE

_____ _____

KEY ADMINISTRATOR 1
Print name Signature

_____ _____

KEY ADMINISTRATOR 2
Print name Signature