

Important Security Information from Personix

At Personix, we take very seriously our responsibility to safeguard the confidential information you share with us. The purpose of this communication is to outline several business practices related to cryptographic key conveyance, key extractions, and the use of keys to calculate card-specific data.

Personix invests millions of dollars to maintain its certification with Visa and MasterCard, insuring the proper equipment is in place to meet or exceed both physical and logical security requirements. Maintaining these levels of security also requires establishing and maintaining appropriate procedures for handling confidential information. Nowhere is this more critical than ensuring the secrecy of cryptographic keys used to personalize cards or to generate PINs.

Due to the risks associated with key-related activities, we cannot deviate from the business practices outlined below. We apologize in advance for any difficulties these procedures may pose to your organization, but trust you will understand our need to adhere to these policies:

1. Sending Keys to Personix.

Personix strongly recommends all entities sending keys to Personix establish a unique Key Exchange Key (KEK) with Personix. Personix cannot accept keys encrypted with a KEK that has already been established or shared with another entity, such as a Zone Control Master Key used to exchange information between your financial institution/processor and Visa or MasterCard.

2. Releasing Keys.

Personix will also require the use of a KEK to process all requests to release keys. The KEK will be used to encrypt the extracted key components prior to forwarding them to the requested entity or individuals. Personix will not extract clear keys under any circumstances. If your financial institution/processor has not already established a unique KEK with Personix, then you will need to allow extra time to secure the required KEK before your key extraction request can be processed. If applicable, fees for KEK creation or key extractions will be disclosed to you at the time you make your request.

3. Clear Keys.

Personix strongly discourages the transmission or communication of any unencrypted (clear) keys to our facilities. This practice is counter to the card associations' recommended practices. Due to the risks associated with potential key compromises, Personix will require entities sending clear keys to execute a waiver of liability, holding Personix harmless for any misuse of those keys.

4. PIN Calculations.

Personix client support and implementation personnel do not have the capability to perform manual or system-generated PIN or CVV/CVC calculations for use in testing, troubleshooting or to address an emergency request for a specific cardholder. We cannot honor requests to manually calculate and communicate PINs via telephone, e-mail, fax, or any other mechanism. Instead, financial institutions will need to establish test cards and should allow time for field testing of plastics to ensure that PIN and CVV/CVC calculations are occurring as expected. For cardholder emergencies, financial institutions should order a PIN via their standard process, and then use the appropriate paperwork to send a request for Rush handling or overnight delivery to Personix.

Our goal in communicating these standards to our clients is to reinforce what has always been true: Personix is committed to providing safe and secure card services to financial institutions, allowing you to focus on building long-lasting relationships with your cardholders. In addition, your data processor will continue to be instrumental in meeting the requirements outlined above.

Thank you for your business. If you have additional questions regarding these policies, please contact Personix Client Services at 866-860-8620 (Personix Indianapolis) or 800-842-4712 (Personix St. Paul).