



# CREDIT AND DEBIT CARD DATA SECURITY PROVIDER COMPARISON CHART

As you are approached by payments processors and data security providers, ask each to answer the following questions. Use this form to document their responses and help determine which solution will best protect your customers' data and your business.

QUESTIONS	HEARTLAND PAYMENT SYSTEMS	PROVIDER #1	PROVIDER #2
Does your solution protect cardholder data from the moment of card swipe or key entry — and through the processor's network — not just at certain points of the transaction flow?	Yes. It is true end-to-end encryption, not point-to-point.		
Does it rely solely on software to protect the data?	No. E3 utilizes both tamper-proof hardware and software because software can be hacked.		
Does it include Tamper-Resistant Security Module (TRSM) hardware?	Yes. E3 devices utilize TRSMs as well as logical protections in the software code.		
Does it leverage Advanced Encryption Standard (AES)?	Yes. E3 uses 128-bit-strong AES — a protocol required by the United States Government and approved by the National Security Agency for top-secret information.		
Does it utilize Identity-Based Encryption (IBE) and Format-Preserving Encryption (FPE)?	Yes. IBE technology ensures E3 devices never have to be "touched" to update the encryption keys. FPE does not alter the format of the data once it is encrypted.		
How are encryption keys managed?	Because with IBE, E3 devices never have to be "touched," cost and administration efforts are reduced and security increased.		
What will I need to do to implement your solution, and what operational changes will I have to make?	Nothing. You don't have to change any of your current business processes.		
When will your solution be available?	E3 devices are available now.		
What will I have to pay up front?	Just purchase an E3 terminal or wedge* at — or below — the prices of standard, less-secure processing equipment on the market today.		
What recurring fees will I have to pay each month?	None. Heartland does not believe you should have to pay more to be secure.		
Does your solution reduce the cost of PCI compliance and risk of being non-compliant?	Yes.		
How will you help me ensure I remain PCI compliant — and what will it cost?	In addition to providing E3 security technology, we help you understand what you need to do to be compliant — like not storing receipts in drawers — at no cost to you.		
Will you help me complete a Self-Assessment Questionnaire (SAQ) specific to my business — and how much will you charge to do that?	Yes — and at no charge.		
Does your solution offer a warranty that will reimburse breach-related fines if my customers' data is compromised?	Yes — with our "E3 End-to-End Encryption Warranty," available at E3secure.com. Reimbursement is subject to the terms and conditions of the warranty.		
Does the processing company behind your security solution subscribe to The Merchant Bill of Rights?	Yes. Heartland believes you have rights. Visit <a href="http://MerchantBillOfRights.org">MerchantBillOfRights.org</a> .		

\* PC-based POS systems may require some integration by your POS provider.



© 2010 Heartland Payment Systems, Inc.

866.941.1HPS (1477)  
HEARTLANDPAYMENTSYSTEMS.COM  
E3SECURE.COM



ho\_E3\_Merchant\_Checklist\_4a - 07.10