StoreNext

Update Bulletin

"Card Data" in PCI-Isolated ISS45 and ScanMaster

January 31, 2008

StoreNext has described the PCI-Isolated payments interface and POS as never seeing, touching, converting, or storing card data. These "PCI-Isolated" POS versions of ISS45 and ScanMaster (with OpenEPS or Connected Payments only!) have been available for about a year now, and most dealers have plenty of experience with multiple installations with these releases.

However, some people were caught off-guard when they just recently noticed that even these isolated POS versions receive – and keep – a few card digits. Isn't that a no-no and contrary to StoreNext's statements about no card data? ***Fair question!***

Here is the fair answer: the reason you can still sleep at night is that ISS45 and ScanMaster meet PCI's black-and-white requirements 100% including what PCI considers "card data." When you're talking about card data, PCI makes the rules, like 'em or not. All resistance is futile.

PCI assumes that it's a good thing for stores to keep a few bread crumbs to follow their transactions back — the first six digits (so the merchant can recognize the card type and BIN) plus the last four digits (to differentiate one account from another). But that's ***all you get!*** That's why OpenEPS guts the rest of the account number before POS sees it. The numbers aren't just "masked" – they're removed and replaced with zeros before they ever hit the POS.

So merchants are left with only those minimum numeric clues they need to manage their stores — these left-over digits that PCI lets you keep are known as "truncated account numbers." Full 16-digit card numbers must be protected, encrypted, masked, cleared etc., and "prohibited card data" (including expiration date, account name, PIN block, CVV2 or any other Track-2 data) can't be kept at all or you'll be posted on Visa's dreaded "Vulnerable Applications List." But certified PCI auditors such as Trustwave — including the three I talked with today — are trained that truncated account numbers are irrelevant when you're looking for bank card data.

So how do you handle a customer who remembers you said "no card data" but notices some digits in the EJ and demands an explanation? Carefully, for starters: you can't expect every grocer to have a PhD in the PCI Data Security Standards. The best straight-up approach is to remind them that (1) the only thing that matters with card data is following the explicit rules in the PCI DSS, (2) the DSS says truncated account numbers are not a problem and (3) our systems provide only the limited numbers that PCI considers necessary and allows.

The final proof will come from any authorized PCI auditor (they actually ***do*** have a DSS PhD) who will certify that the grocer is in the clear. Don't be shy about giving your customers a copy of the DSS — we always keep the current version on-line — and the more they understand, the more they understand the value you're bringing. It shows exactly where PCI drew the line.

And that you're squarely on the right side of it.

Antony van Seventer