StoreNext

Update Bulletin

Visa Compliance Questions and Answers

June 6, 2005

Here are the key questions and answers about "Visa Compliance," PCI and CISP.

WHO ARE THESE GUYS?

I'm hearing about this "Visa Compliance" thing: half my customers are in a total panic and don't know what to do and the other half are just clueless - and don't know what to do. Who's making the rules, here? — Visa is making the rules. With their enormous share of the credit processing market, they are in a position to drive the regulations on processing, and they also have the most to lose through credit card fraud or consumer distrust of the safety of using Visa cards.

What are "CISP" and "PCI"? — In 2001, Visa implemented the "Cardholder Information Security Program". CISP provides a set of tools, standards and measurements, and "CISP Compliance" is required of all processors and merchants involved in handling Visa transactions. Meanwhile, Visa and MasterCard collaborated to create the "Payment Card Industry (PCI) Data Security Standard". CISP compliance mandates that the PCI standards be followed.

What are these PCI standards about? — The PCI standards describe what card processors and merchants need to do in a number of areas, including how they must keep their networks (with payments data) secure, how they must maintain a clear security policy, protect cardholder data, implement anti-virus and other security systems, restrict access to this data and track / test their system regularly.

Who says that someone meets the standards or not? — Visa has set up a Compliance Validation system, designed to find vulnerabilities and define corrective action. One set of standards is used by payments processors while the other is set up for merchants. This system relies heavily on questionnaires and audits to be carried out by the merchants and qualified consultants.

WHO'S AFFECTED?

Where do my grocery customers fit in this scheme of things? — It depends on their "level" within the CISP scheme. But it's safe to say that just about any independent grocer will be in the lowest, most lenient level — "Level 4". Specifically, a grocer who processes less than 6,000,000 Visa transactions per year will normally be at this lowest level of compliance requirements. To give you an idea of how this works out, if the average Visa transaction in the store is $40, and the grocer processes 20% of their transactions through Visa, then the company would need to have annual revenues of about $1.2 billion to be other than Level 4, unless special conditions apply (normally these conditions are unlikely to apply to a grocer, such as large volumes of *e*-commerce Visa transactions, e.g. Amazon.com).

What are my grocery customers supposed to do? — Assuming they're in Level 4, the regulations currently recommended that they annually carry out an annual self-assessment questionnaire regarding their compliance with the PCI standards. It is also recommended that they have a

"network scan" carried out by a qualified independent consultant to determine risk on their networks. There is currently no specific date that Visa has set that mandates this activity for Level 4 merchants.

No date? What's all this about June 30, 2005? — June 30 is the date by which Level 3 and Level 2 merchants are required to perform the self-assessment questionnaire and network scan mentioned above. Level 1 participants were to have done this in September of 2004.

So who is all this Visa Compliance stuff aimed at? — According to consultants and industry experts, the initial target of the PCI standards has been but the "member" financial institutions and processing networks. This is where the volume of transaction information is concentrated and considered most vulnerable to fraud on a massive scale. It would naturally be far more concerning if financial institutions and payments processors were being hacked than Pete's IGA.

REAL-LIFE IMPACT FOR THE INDEPENDENT

So is Pete's IGA off the hook? — No, they're not off the hook at all. Once you get off the pages of the Visa USA Operating Regulations and into real life, here's how it works:

- Visa has contracts with First Data and other processors and "member" financial institutions. These members and processors have a separate scheme of CISP regulations requiring on-site audits etc. (these were required for completion in September 2004).
- As processor contracts with Visa have come due for renewal, Visa has written conditions into these contracts that require CISP compliance.
- Members are not only considered responsible for their own security and compliance, but also the CISP compliance of their merchants. Visa makes members directly responsible for any liability that arises out of non-compliance from their merchants.
- Members must also include CISP-compliance provisions in all their merchant contracts. So when Pete's agreement comes up for renewal with their network or bank, the CISP-compliance requirements are certain to be there.

How is all this enforced? — Under the contractual obligations, Visa can fine the members and processors up to $500,000 for any incident where one of their merchants isn't CISP-compliant, and doesn't rectify security issues or has a security breach. Not only can Visa fine the acquiring member institution, but they can reach down and put restrictions on the merchant or ban that merchant from participating in Visa programs.

If my grocer is CISP-compliant, are they protected? — Yes, according to the published rules, if a merchant is CISP-compliant, then the member / processor is protected from fines. The grocer's own contract with the processor would reflect the same protections under the CISP rules — the processor wouldn't be able to fine the grocer so long as the grocer is CISP-compliant.

And if the grocer is not CISP-compliant? — They are subject to all those fines and penalties depending upon their contract.

But isn't there a "grandfather clause"? Something like they don't have to worry about the regulations until they buy a new POS system? — There do not appear to be any such "grandfather clauses" in the CISP system that would allow a merchant to wait until a new system purchase before having to meet the regulations. It's all driven by the merchant's contract with the processor.

RULES THAT DIRECTLY IMPACT POS

Weren't there some standards in place anyway? — CISP data standards have become more stringent over time. Earlier rules prohibited stores from allowing account numbers, expiration

dates, PINs etc. to leave the store. That means that this data must be masked on the receipt. In the store, any copies of charge slips or paper items that have this account data must be locked away so that only authorized staff with a need to know may access them. Any such data in the store's computers must be password protected.

But there is more, right? — Yes. The stricter compliancy requirements prohibit merchants from storing certain key cardholder data in any form. It also means that store logs and files, including the electronic payments systems, cannot retain some of this data. This can impact T-Logs, for example, and POS electronic journals that normally are able to read such data out — this will no longer be allowable.

Can't stores just encrypt or mask the data? — No. Some account data can't be there at all, even in encrypted form. The best practice is for it not to be there at all.

How can a store check which card was used for a previous transaction — for example to put a refund or credit onto the right card account? — The rules allow you to keep the first and last few digits of the credit card number – this will allow the merchant to recognize which card was used, but without having any way of reconstructing the full number. For example, the ISS45 system will keep the first six digits and the last four digits, and all the rest of the numbers will be set to zero. This meets the requirements for security since is no practical way of guessing what the missing six digits might be. But the grocer could still check that remaining data against a shopper's credit card to be sure they're refunding the right account.

Strictly speaking, how can you even run a payments transaction if you can't "store" the data? For example, what if you're off-line? — You're right: technically, any system has to know — even if just momentarily — the account data if it's going to be able to process a transaction. Furthermore, off-line / store-and-forward transactions would require retention of the data until the transaction can be completed.

So how's it supposed to be done? — The CISP rules address this by stating that a merchant or system can store the information while a transaction is "in-process". So, for example, the electronic payments system can hold onto that data in cases where store-and-forward is required until the transaction is completed. Once completed, however, that data must be destroyed.

COMPLIANT RELEASES AND NEXT STEPS

Which StoreNext systems are affected by these rules? — Both ISS45 and ScanMaster are affected since they handle shopper account data. RBO, TCI, PocketOffice and ESL are not affected. U-Scan is largely driven by the underlying POS and is compliant.

What about Connected Services? Doesn't it take T-Log data from the store up to the Connected Services database? — Since the updated system T-Logs for ISS45 and ScanMaster will not have account data, Connected Services will no longer receive such information from the store once compliant POS is installed. In addition, Connected Services is scheduling a filter to prevent non-compliant data as well as a one-time card-number "overwrite" to ensure that grocers' data at Connected Services meets compliance specifications.

What's the status of ScanMaster and of ISS45? — The compliance table is provided below, providing the releases that are compliant with the current "masking" requirements and the more stringent "data" requirements.

Product and Version	"Masking" Compliance	"Data" Compliance
ScanMaster V1	1.02.03	1.3.0-060
ScanMaster V2	2.1.2-060	2.2.0-050
ISS45 V7	7.0.9.0-050	7.1.0.0-060
ISS45 V8	8.1.0.0-050	8.1.0.1-050

Should grocers implement these new releases? — Yes, since audits will indicate that these releases are required to meet the standards.

When will the latest releases be available? — StoreNext posts the ISS45 and ScanMaster RoadMaps on the StoreNext Dealer Support Web site.

Will StoreNext go back and retrofit other ISS45 releases, such as 7.6, 7.7.1, 8.4.3 and so forth? — The engineering effort that would be required to rewrite old software releases around the new system data storage, T-Log and journaling standards is prohibitive and cannot be practically undertaken. If the store software will need to be upgraded regardless, it also may as well be to the current release.

If a dealer needs to upgrade ScanMaster systems what should they do? — StoreNext ScanMaster dealers can upgrade their users to Visa Compliant releases of either V1 or V2 by ordering the no-charge upgrade to the compliant StoreNext V1 or V2 releases from StoreNext. This will provide the necessary licenses and keys for the upgrade.[1]

How will dealers get the updated ISS45 releases? — ISS45 Version 8.1.0.1-050 is planned for release this month, June 2005 and will be delivered to dealers in good standing via CD-ROM. The 7.1.0.0-060 will be loadable over the 7.1.0.0-050 CD-ROM that will be in your hands shortly.

How can I get copies of the actual Visa documents, surveys and standards so I can see for myself? — StoreNext has implemented a new "Visa Compliance" Page on the StoreNext Dealer Support Web site, accessible from the left-hand Menu or the Software Support Page. You'll find this bulletin, plus a number of the official payments industry documents, including the PCI Standards, the Self-Assessment Questionnaire, Best Practices and so forth.

How about something I can hand my customers? — This must be one of those good days. First, you have answers to a lot of questions, a resource for more information, upgraded software that's compliant — and free — plus a StoreNext Sales Sheet to help you with your installed base. See the Brochures Page on the StoreNext Dealer Support Web site.

To Your Success

Anton van Sevenster

[1] ScanMaster license upgrades to the StoreNext versions are currently available at no charge for the application only — any platform, operating system, database etc. costs are not included in the ScanMaster application license.