



PCI and Visa CISP Compliance

WHAT THESE STANDARDS MEAN TO THE INDEPENDENT GROCER AND REGIONAL CHAIN — AND HOW STORENEXT HELPS YOU MEET THEM.

The Payments Card Industry has always had requirements and standards, and here's what you need to know about the current PCI mandates.

To protect cardholders, businesses and the payments card industry itself, regulations have been enacted that mandate changes in the way payment card information is used and handled.

In 2001, Visa implemented “CISP” – the Cardholder Information Security Program. CISP provides tools and standards, and “CISP Compliance” is required of all processors and merchants involved in Visa transactions.

Meanwhile, Visa and MasterCard collaborated to create the Payment Card Industry (“PCI”) Data Security Standard. Visa CISP compliance mandates that merchants meet PCI standards.

The PCI Data Security Standards (“DSS”) describe how retailers must keep card data and 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.

Visa has also developed a Compliance Validation system, relying heavily on questionnaires and audits to be carried out by the merchants and qualified consultants.

The following questions and answers provide information on some of the key components of these compliance standards.

How is my grocery business part of this set of requirements? Your compliance requirements depend on your merchant “level” within the CISP scheme. Most independent grocers will be in “Level 4.” Grocers who process less than 1,000,000 Visa transactions per year will be at this lowest level of audit requirements.

If I'm in Level 4, does that mean I don't have to do anything? The CISP requirements for auditing and so forth are more lenient for Level 4 grocers, but all merchants must still be PCI compliant.

How will my requirements be documented to me? These will come to you via your pay-

ments processor, often with your payments contract renewal.

Why will it come from my processor? PCI compliance is enforced through the card associations' member processors and financial institutions. As these members' contracts have come due for renewal, Visa, MasterCard and others have written conditions into these contracts that require PCI compliance.

So these processors are the ones that are really responsible for compliance? Visa makes member processors directly responsible for any liability that arises out of non-compliance from their merchants. So Visa requires that members also include CISP/PCI compliance provisions in all their contracts with merchants.

Are these requirements in my current contract? Depending upon when it was executed, that's certainly possible – and by now even likely. When your processing agreement next comes up for renewal with your network or bank, however, the CISP-compliance requirements are certain to be there.

How are the requirements enforced? Visa can fine members and processors up to \$500,000 for any security incident or breach where one of their merchants isn't CISP/PCI compliant and/or doesn't rectify security issues. Visa also can reach down and place restrictions on merchants, or ban merchants from participating in Visa programs.

If I'm compliant, am I protected from these penalties? Yes, according to the published rules, if a merchant is CISP/PCI compliant, then the member/processor is protected from fines. The grocer's own contract with the processor would reflect the same protections under the rules – the processor wouldn't be able to fine the grocer so long as the grocer is compliant.

But if I'm not compliant? You would be subject to all those fines and penalties depending upon your contract with your processor.

But isn't there a "grandfather clause"? Something so I don't have to worry about meeting these requirements until, say, I get a new POS or payments system? There are no "grandfather clauses" in CISP that provide relief from the requirements.

Weren't there some standards in place anyway? CISP/PCI data standards have become more stringent. Earlier rules prohibited stores from allowing receipts with account numbers, expiration dates, PINs, etc., to leave the store – so this data must be "masked." In the store, any copies of charge slips or paper items that have this account data had to be locked away so that only authorized staff with a need to know could access them. And any such data in the store's computers were required to be password protected.

But aren't there newer requirements with additional restrictions? Yes. The more stringent compliance requirements prohibit merchants from storing certain card data in any form. Data logs and files, including electronic payments systems, must normally be encrypted and can retain partial information for only a limited time and be password protected.

Which StoreNext systems are affected by these rules? Both ISS45 and ScanMaster were initially affected since they handled shopper account data. WinEPS has passed all PCI audit processes. U-Scan is largely driven by the POS and complies. RBO, Retailix Store ("TCI"), PocketOffice and ESL are not affected. Connected Services has made all data compliant.

What about "PCI Isolation"? New releases of ISS45 and ScanMaster, when used with up-level WinEPS, never handle or process any card data whatsoever. These systems are therefore isolated from PCI concerns regarding card data security.

Does StoreNext Connected Payments help with PCI? Yes, since with this system all card data resides at fully-compliant data centers. With a "PCI-Isolated" POS and Connected Payments, no card data remains in the store, removing the store from all requirements with the exception of the audit questionnaire.

Should grocers install these new releases? Yes, since they will limit compliance costs or be required to meet established standards.

Will StoreNext go back and revise other ISS45 and ScanMaster releases? The effort required to rewrite old software releases to new PCI standards is prohibitive and cannot be practically undertaken.

PCI COMPLIANCE STATUS SUMMARY

The PCI compliance table at right shows the POS software, WinEPS, Concord and Connected Payments releases and compliance levels.

PCI COMPLIANCE STATUS SUMMARY			
PRODUCT AND VERSION	PCI ISOLATION	"DATA" COMPLIANCE	"MASKING" COMPLIANCE
ScanMaster V1	N/A	1.03.00-060	1.02.03
ScanMaster V2	2.04.01-050	2.02.00-050	2.1.2-060
ISS45 V7	7.1.2.0-050	7.1.0.0-060	7.0.9.0-050
ISS45 V8	8.1.2.0-050	8.1.0.1-050	8.1.0.0-050
WinEPS & I/F	820.2	816.1	813.0
Concord I/F (2001+)	N/A	Yes*	Yes*
Connected Payments	All	All	All

*Assuming use with compliant POS and payments software



WHERE EVERY DAY IS INDEPENDENTS' DAY

6100 TENNYSON PARKWAY, SUITE 130 | PLANO, TEXAS 75024

800-298-0151 www.storenex.com