PCI and Visa CISP Compliance

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

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

StoreNext

To protect businesses, cardholders 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.

Visa and MasterCard also created the Payment Card Industry ("PCI") Data Security Standard. Visa CISP compliance mandates that merchants meet PCI standards.

The PCI Data Security Standard ("DSS") describes how retailers must manage card data and networks that transport this data. A security policy must be maintained that restricts access to cardholder data, implements anti-virus and security systems, and regularly scans networks for potential intrusion points.

PCI 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 affected by these 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? Even Level 4 grocers must complete the Self-Assessment Questionnaire (SAQ) and complete quarterly network scans.

How will my requirements be documented to me? These will come to you via your payments processor, often with your payments contract renewal. PCI information is also always available on Visa's Web site.

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? Almost all current processing contracts require PCI compliance, and those that don't will include these provisions when next renewed.

How are the requirements enforced? Visa can fine members and processors up to $500,000 for any security incident or breach where a merchant isn't CISP/PCI compliant and/or doesn't rectify security issues. Visa also can reach down and demand on-site audits, 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, compliant merchants and their processors will not be fined.

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

Can PCI protect me from lawsuits in case of a breach? Although maintaining compliance supports a merchant's claim of diligence protecting cardholder data, PCI is outside the legal system and does not limit civil or criminal proceedings.

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" that provide relief from PCI 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. These more stringent requirements forbid merchants from storing certain "prohibited data" such as PIN blocks, card verification numbers or expiration dates. Account numbers should be encrypted and under password protection, and may only be retained for a limited time.

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

What about "PCI Isolation"? When used with Connected Payments or WinEPS, newer releases of ISS45 and ScanMaster are isolated from any full account data and see only "truncated" numbers. Under PCI rules, these POS releases are therefore not considered "payment applications" for assessment and listing on the Visa Web site.

Does StoreNext Connected Payments help with PCI? Yes, since Connected Payments stores all card data at fully-compliant data centers instead of the merchant's store. So in combination with a "PCI-Isolated" POS and Connected Payments, no true card data remains in the store. This exempts the merchant from most PCI remediation costs and greatly simplifies achieving and maintaining compliance.

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[1]	2.02.00-050	2.1.2-060
ISS45 V7	7.1.2.0-050[1]	7.1.0.0-060	7.0.9.0-050
ISS45 V8	8.1.2.0-050[1]	8.1.0.1-050	8.1.0.0-050
WinEPS & I/F	820.2[2]	816.1	813.0
Concord I/F (2001+)	N/A	Yes[4]	Yes[4]
Connected Payments	All[3]	All	All

1 Requires WinEPS 820 or later
2 Requires PCI-Isolated version of ISS45 or ScanMaster above
3 Requires PCI-Isolated version of ISS45 or ScanMaster above and OpenEPS "client/direct" implementation at POS
4 Assumes use with compliant POS and payments software

StoreNext
WHERE EVERY DAY IS INDEPENDENTS' DAY
6100 TENNYSON PARKWAY, SUITE 130 | PLANO, TEXAS 75024
800-298-0151 www.storenext.com