

DIEBOLD AND PCI DSS



Implementing PCI DSS requirements helps proactively protect customer data against fraud.

The Payment Card Industry Data Security Standards (PCI DSS) is a set of requirements developed by the PCI Security Standards Council for addressing the security of cardholder data that is stored, processed, or transmitted.

PCI Security Standards Council members are: MasterCard, Visa, American Express, Discover Financial Services and JCB International.

This standard was created to help facilitate the adoption of strong and consistent data security measures to help protect sensitive cardholder data using a POS, e-commerce and also ATMs. It covers all aspects to protect customer sensitive data such as security management, policies, procedures, network architecture, software design and other critical protective measures. It is a set of comprehensive requirements for safeguarding cardholder's sensitive data.

PCI DSS at a glance

PCI Data Security Standards (DSS) addresses the security of cardholder data that is stored, processed, or transmitted. The PCI Council has defined and specified a set of requirements that merchants and service providers manipulating such sensitive data have to implement.

PCI DSS defines a set of 12 requirements which address six main areas:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI DSS requirements

• *Build and Maintain a Secure Network*

1. It is required to install firewalls to control the traffic permitted and to block any other unsecured communications. This protection mechanism allows blocking any unauthorized access from the internet.
2. Maintaining a secure network requires also changing default passwords and security default settings that hackers may know.

• *Protect Cardholder Data*

3. This area requires the encryption of cardholder data so that any intruder having access to encrypted data cannot use it without having cryptographic keys. It also requires that sensitive cardholder data such as full magnetic stripe, authentication data or PIN data are not stored. The truncation of cardholder data, if full PAN is not needed, is also required.
4. Cardholder data must be encrypted when transmitted across open and public networks.

• *Maintain a Vulnerability Management Program*

5. The vulnerability management program requires the use of anti-virus software with periodic updates of virus patterns for protecting sensitive data against frauds.
6. The security of systems and applications must be maintained by making sure the most recent software

security updates and patches are installed to address vulnerabilities that unscrupulous persons could use to exploit and compromise cardholder data.

Computer networks and the Internet are an emerging target for financial frauds. Insufficient security by some merchant or service providers enables criminals to capture sensitive customer account data and to use it for financial frauds. PCI DSS helps protect sensitive cardholder data and reduces the vulnerabilities found in all card processing systems.

• *Implement Strong Access Control Measures*

7. The first measure is to strictly limit access to sensitive cardholder data to authorized individuals whose job responsibilities require such access.

This requires implementing an access control system to restrict access to authorized individuals only.

8. One unique ID must be assigned to each person to access cardholder data.
9. Any physical access to cardholder data must be controlled and restricted as appropriate to prevent unauthorized access to devices or to get information on critical data.

• *Regularly Monitor and Test Networks*

10. Utilizing logging mechanisms to track user activities is essential in preventing, detecting, or minimizing the impact of cardholder data compromise. Maintaining log files in all environments allows tracking and provides the capability to set alerts to analyze any potential issues as well as determining the origin of the issue.
11. New vulnerabilities are periodically discovered and introduced in new software. It is important to regularly test systems, software and processes to ensure that security controls are adaptive in a rapidly changing environment.

• *Maintain an Information Security Policy*

12. It is required to maintain a company-wide security policy and inform all employees of these measures and their responsibilities in protecting sensitive data. This includes contractors, consultants and temporary employees who have access to the company's site.

Assessment for Compliance with PCI DSS Requirements

Any network component (firewalls, switches, routers, wireless access, appliances, etc.), any server (Web, applications, databases, authentication, DNS, etc.) and any application (third party, custom, embedded or external such as Internet applications, etc.) that manage cardholder data are to be included in the PCI DSS assessment for compliance. This defines the cardholder data environment.

In some cases, network segmentation of the cardholder data environment can be considered with the assessor to reduce the scope, difficulty and cost of the PCI DSS assessment. Network segmentation for PCI DSS assessment can be achieved through internal network firewalls or routers provided there are strong methods that restrict access.

All ATM software components dealing with customers' data are involved in a PCI DSS compliance assessment as none of them can violate PCI DSS requirements. This is the reason why Diebold has audited all software pieces running on Diebold ATMs and applied changes required to not violate applicable PCI DSS requirements.

How to Comply with PCI DSS

PCI DSS compliance is expected for merchants, and more generally, for any organization that process, transmit or store cardholder data.

Enforcement programs may vary depending on the card acquirer with specific requirements for validation and reporting (e.g. Qualified Security Assessor (QSA) or Self-Assessment).

Cardholder Data is defined as the data elements contained in the card (chip, magnetic track, printed on the card) such as Primary Account Number (PAN), cardholder name, service code, expiration date. Sensitive Authentication Data are full magnetic stripe data, CAV2 / CVC2 / CVV2 / CID, and the PIN Block.

Qualified Security Assessor

A QSA is a data security company certified by the PCI Council which is accredited to perform assessments on site for PCI DSS compliance and produce the report on compliance (ROC).

Approved Scanning Vendor

An Approved Scanning Vendor (ASV) is a data security company focusing on validating the compliance with the PCI DSS external vulnerability scanning requirement. ASV's may submit ROC to the acquirer on behalf of a merchant or service provider.

Self-Assessment Questionnaire

For merchants and service providers who are not required to perform an on-site assessment, the Self-Assessment Questionnaire (SAQ) is a PCI DSS tool allowing the performance of self-validation for PCI DSS compliance. It includes questions for compliance. There are five types of SAQ adapted to the type of merchants or service providers.

Reporting

Merchants and organizations verify on-site PCI DSS compliance to acquiring financial institutions by means of ROCs. SAQ or annual attestations may be required depending on the acquirer requirements. Scanning reports can also be required on a quarterly basis. PCI DSS reports include findings, business information, infrastructure description and external dependencies.

Third Parties/Outsourcing

For merchants and service providers outsourcing processing, storage or transmission of cardholder data, or management of routers, firewalls, servers, physical security, etc., the ROC must include each respective role and identify what PCI DSS requirements apply to these third party service providers.

To validate compliance, these third-party providers have the option to:

- Undergo a PCI DSS assessment on their own and provide evidence to their customers they comply
- Have their services reviewed during their customer's PCI DSS assessment

Customer Sensitive Data Stored on Diebold ATMs

There are three main areas in a modern ATM where sensitive data is collected and stored. These areas include the electronic journal file, the communication software and the trace/log files for debugging and support purposes. Each of these areas that manage cardholder data have to meet PCI DSS requirement 3, related to protecting stored cardholder data.

The most important requirements for ATMs are requirements 3 and 4 which are related to customer sensitive data protection that are stored locally and transmitted across the network.

Electronic journal file

The electronic journal file contains a combination of data provided by both the ATM and the ATM driving host and is required for business use. Host data sent to the ATM to be partially printed on the receipt is captured in this file for later use in reconciliation of disputes. For that reason it traditionally contains the customer account number and transaction information. This data exists as a string of text data and the ATM simply records it to the file. The ATM has no knowledge of the context of the data and cannot edit or mask this data. In rare instances when a card is retained by the ATM's card reader, an entry is made on the journal of the track 2 data of that card. This is intended to facilitate customer service by helping verify which cards were actually retained.

Communication software

The communication layer is the software module used to communicate data between the ATM and the ATM driving host. This module has an optional tracing facility within it to capture data for debugging and support purposes. When enabled, this tracing facility captures cardholder data among other data. The communication software is message format agnostic. This means that this communication module does not know the semantic of data exchanged between the ATM and the ATM driving host, and therefore does not know where cardholder sensitive data are located in the messages.

In addition, Diebold Communication Software offers SSL encryption at the ATMs for addressing PCI DSS requirement 4: Encrypt transmission of cardholder data across open, public networks. This solution allows for all ATM transactions to be encrypted from the ATM to a Cisco ACE bridge or to an ATM host that supports SSL communication.

Log processing

Log files capture the activity and exchanges of data between ATM devices and the ATM processor. These contain vital information regarding the health and performance of the hardware and the software. In cases of the card reader and encrypted PIN pad, the data that contains the information provided by the module is recorded. However, in no instance is an

unencrypted PIN or an encrypted PIN block recorded. The PIN is never visible in its unencrypted format as encryption is addressed inside the PIN pad.

Log processing is a complex maintenance program that runs on the ATM 24 hours a day and must perform its functions while being invisible to the consumer and host processor alike. Log processing is actually more like a collection of applications running at various times collecting different data.

Diebold and PCI DSS

Diebold is committed to the security of financial transactions and we constantly monitor and make improvements to our software, processes and procedures to eliminate vulnerabilities and comply with industry regulations.

Addressing PCI DSS requirements does not require any hardware upgrade on the ATM side. Diebold ATMs provide the most recent technologies for ensuring highest level of security (including Encryption keys, encrypted PIN pad, anti-skimming card readers, EMV, firewall, etc.) and for protecting values that are deposited or delivered (notes, checks, coins, etc.).

Diebold is making PCI DSS improvements to the most common Diebold software products and services based on Windows® XP Pro. For older product releases and services, Diebold recommends that our customers move to a more recent solution compatible with PCI DSS. No PCI DSS improvements are planned on former OS/2, Windows® NT, Windows® 2000 and Windows® XPe based Diebold products.

Software products and services that are planned to address PCI DSS requirements are listed below:

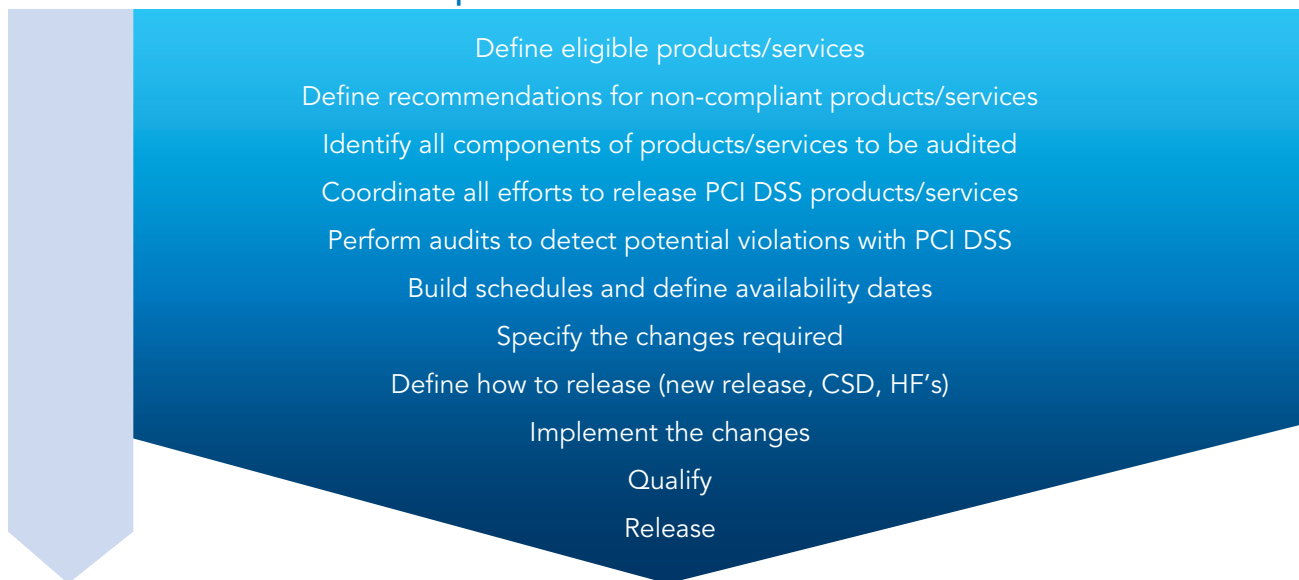
PRODUCT / SERVICE PCI DSS READY	MINIMUM VERSION LEVEL
Agilis 91x XV	Release 2.3.1 or higher
Agilis ix/CSP	Release 1.6.3 or higher
Agilis NDx XV	Release 2.1.1 or higher
Agilis EmPower	Base: Release 3.2 SP2 or higher Maintenance: Release 2.0 or higher NDx plug-in: Release 1.2 SP1 or higher 91x plug-in: Release 3.0 or higher IFX plug-in: Release 1.3
Agilis XFS	Opteva: Release 3.6.2 or higher Ix: Release 1.40.1 or higher Ix: Release 3.2 plus Hot Fix or higher 9x Series: Release 3.2.1 or higher
INvolve	Release 3.8 SP1 plus Hot Fix or higher
EMV Kernel	Release 4.1 plus Hot Fix or higher
Agilis Base Communication	Release 4.4.0 or higher
Diebold Data Transfer (formerly DTS/DTC)	Release 5.1 or higher
ImageWay ATM (RSS)	ImageWay ATM 2.5.1 or higher
Power Extension	Release 2.3 or higher
Security Office	Release 9.12 or higher
Journal Office	Release 1.5 or higher
Campaign Office	Release 3.2 or higher
Remote Office	Release 10.0 or higher
OneTouch	N/A
Opteview	Release 5.2 or higher
SNMP Agent	N/A
Mayfair software	Release 3.0 or higher

Diebold recommends that older software products/services migrate to a PCI DSS ready replacement solution when required by acquirers as indicated in the migration table below:

NON PCI DSS PRODUCT / SERVICE	RECOMMENDED REPLACEMENT SOLUTION
Agilis 91x Opteva (all versions)	Agilis 91x XV Release 2.3.1 or higher
Agilis 91x for D450	Planned Agilis 91x 3.1
Agilis 91x for D620	TBD
Agilis NDx Opteva Releases 1.1 to 1.4	Agilis NDx XV Release 2.1.1 or higher
Agilis Power – all versions	Agilis EmPower Base: Release 3.2 SP2 or higher
Agilis XFS 9x CEN 2.0 based releases	Agilis XFS 9x Series CEN 3.0 Release 3.2.1 or higher
IqESD/iqCRM	Office suite product

To address PCI DSS requirements, Diebold has developed a process to help ensure that all Diebold solution components that manage sensitive cardholder data address PCI DSS requirements for protecting data.

Steps for Diebold to address PCI DSS



Glossary

ASV Approved Scanning Vendor
ATM Automated Teller Machine
CSD Corrective Service Disk
DSS Data Security Standard
EPP Encrypted Pin Pad
HF Hot Fix
ICC Integrated Circuit Card
LAN Local Area Network
PAN Primary Account Number
PCI Payment Card Industry

PED PIN Entry Device
PIN Personal Identification Number
POS Point Of Sale
QSA Qualified Security Assessor
ROC Report On Compliance
SAQ Self-Assessment Questionnaire
SSL Secure Sockets layer
WAN Wide Area Network

PCI DSS getting started

1. What is PCI?

The PCI SSC (Payment Card Industry Security Standards Council) is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.

2. What is PCI DSS?

PCI DSS is a standard specified by the PCI Security Standards Council for protecting customer's sensitive data.

3. What is the aim of PCI DSS?

The aim of PCI DSS is to create a recognized worldwide standard and to facilitate the adoption of security measures to protect customer's sensitive data.

4. What aspects covers PCI DSS standard?

PCI DSS covers the security management, policies, procedures, network architecture, software design and protective measures to protect customer sensitive data.

5. What PCI standard exists in addition to PCI DSS?

PCI Security Standards Council issued in 2005 the PED (PIN Entry Devices) standard for Encrypting PIN Pad (EPP) and in 2008 the Payment Application Data Security Standard (PA-DSS), formerly known as Payment Application Best Practices (PABP).

6. Why PCI DSS is so important?

Computer networks and the Internet are an emerging target for financial frauds. Insufficient security by some merchant or service providers enables criminals to capture sensitive customer account data and to use it for financial frauds. PCI DSS helps protect sensitive cardholder data and reduces the vulnerabilities found in all card processing systems.

7. What is the current version of PCI DSS standard?

Current version of PCI DSS requirements and procedures specification is version 1.2 released in October 2008. Version 1.2 is a revision of the version 1.1 that provides clarifications on requirements and procedures. There is no new major requirements in version 1.2 impacting ATM's. It provides clarification on requirements and

procedures. All new PCI DSS assessments started or to be started after Dec. 31, 2008 must be conducted using version 1.2.

8. How does PCI DSS define Cardholder Data and Cardholder Sensitive Data?

From a PCI DSS standpoint, cardholder data is defined as the data elements contained in the card (chip, magnetic track, printed on the card) such as primary account number (PAN), cardholder name, service code, expiration date. Sensitive authentication data are full magnetic stripe data, CAV2 / CVC2 / CVV2 / CID, and the PIN Block.

PCI DSS defines rules for storage and protection for each of those data. One of the most critical is the PAN for which PCI DSS requires to render, at minimum, unreadable anywhere it is stored.

9. What does "Merchant" mean for PCI DSS?

PCI DSS defines a merchant as an entity accepting payment cards of the five members of the PCI Council – American Express, Discover, JCB, MasterCard, Visa – for payment.

10. Who mandates the PCI DSS compliance?

Compliance is mandated by the payment card brands and not by the PCI Security Standards Council. Each individual payment brand is responsible for managing and enforcing compliance to this standard.

11. What is the deadline for complying with PCI DSS?

Compliance is mandated by the payment card brands. Merchants and service providers have to check with their acquirers what deadline is required.

12. When will be the PCI DSS standard mandatory?

Full implementation of PCI DSS depends on the country and on the network authority involved.

13. Is the PCI DSS standard for US only?

No, PCI DSS is a global standard that applies to any country that sources, processes or transfers cardholder data.

PCI DSS and Diebold ATMs

14. Are all requirements applicable to ATMs?

ATMs are one component of the bank infrastructure for performing banking transactions and represent a portion of the cardholder data environment. They must comply with PCI DSS requirements that apply for ATM components. The most important requirements for ATMs are requirements 3 and 4 which are related to customer sensitive data protection that are stored locally and transmitted across the network.

15. Do Diebold ATM software already address PCI DSS requirements?

Some software pieces already address the PCI DSS standard and the software solution components that do not are being adapted to address PCI DSS requirements. These efforts are geared to protect and prohibit the storage of customer's sensitive data.

16. What does the PCI DSS effort consist of for a Diebold ATM?

The following steps were defined for ATM software and services to comply with PCI DSS standards:

- Define eligible products/services
- Define migration recommendations for non PCI DSS products/services
- Perform internal audits on products/services to detect potential violations with PCI-DSS requirements
- Identify all components to be checked for a product or service solution
- Specify and implement the changes required
- Coordinate all efforts to release compliant products/services
- Define how to release - New release, CSD (Corrective Service Disk), Hot Fixes (HF's)
- Implement and qualify
- Release

17. What is the Diebold plan for providing customers with PCI DSS solutions?

The initiative started in early 2008.

The plan consists of the following steps:

- Start the PCI DSS program
- Coordinate all impacted development teams
- Identify products/services to comply with PCI DSS
- Define migration recommendations for older solutions
- Start audits and identified components requiring changes
- Start implementing changes in products/services
- Complete qualification
- Release PCI DSS software products and services

18. Which parts of the ATM require an upgrade?

Addressing PCI DSS requirements does not require any hardware upgrade on the ATM side. Diebold ATM's provide the most recent technologies for ensuring highest level of security (including encryption keys, EPP, anti-skimming card readers, EMV, firewall, etc.) and for protecting values that are deposited or delivered (notes, checks, coins, etc.).

Only those Diebold software solutions and services that are being improved to address PCI DSS requirements will require an upgrade on the installed base.

19. What kind of PCI DSS upgrade is or will be proposed by Diebold?

Upgrade for existing software products and services will be achieved mainly by means of CSDs. Those CSDs may also include SCR's for quality improvements as for any CSD.

In addition to upgrades, there will be some cases where Diebold will provide our customers with documents describing recommendations on how to use particular software or service in a manner that complies with PCI DSS requirements.

20. Will all Diebold software and services address PCI DSS requirements?

Diebold will provide improvements for PCI DSS for most recent software products and services, which is not limited to last versions of software. However, old software products and services will not be improved. Contact your local sales representatives for more information on what products/services and versions will fit your needs.

21. What does PCI DSS mean for a Diebold software solution?

A Diebold software solution is composed of many software products and services. PCI DSS requirements are met on the ATM side when all components of the solution address applicable requirements (e.g. XFS, INvolve middleware, Communication software, Application software, EMV kernel, monitoring system, file transfer, etc.).

Installing one piece of software that violates PCI DSS requirements with all others software pieces would result in a non-PCI DSS overall ATM solution.

22. Is there any case where an unencrypted PIN is stored on the hard drive of the ATM?

No. In no case is an unencrypted PIN recorded in any

log or trace file. The PIN is never visible in its unencrypted format as encryption is addressed inside the EPP pin pad.

23. How will Diebold deliver “PCI DSS ready” solutions to customers?

Most current software products will have a CSD for adding PCI DSS support and can be installed on existing installed software provided they are eligible for these CSDs. New Diebold software products/services will natively address PCI DSS applicable requirements (e.g. Agilis 91x v2.4).

PCI DSS Validation

24. What system modules are involved in PCI DSS assessment?

A PCI DSS assessment takes into account all components and behaviors of the card transaction, from end to end, from POS, e-commerce application, ATMs, to servers, and include network, switches and service providers.

This means ATMs are a subset only of the transaction process to be assessed.

25. What is the scope of the PCI DSS assessment?

The scope of the PCI DSS assessment includes the entire network.

To aid in reducing the cost of assessment and the challenges of implementing and maintaining PCI DSS controls, network segmentation can be achieved with firewalls, routers or any other method restricting access to that segment. The assessor must verify however, that the proposed segmentation is adequate to reduce the scope of the PCI DSS assessment.

26. Which types of certification have to be achieved by an ATM before it can be considered PCI DSS compliant?

There is actually no formal PCI DSS “certification” for single ATMs. Card acquirers require merchant and service providers to provide Report On Compliance (ROC) once a PCI DSS assessment is complete. The assessment can be performed on-site by a Qualified Security Assessor, an Approved Scanning Vendor (ASV) or by means of Self Assessment Questionnaire (SAQ), depending on the card acquirers’ requirements.

For the ATM portion, the PCI DSS compliance verification is part of the merchant or service provider global assessment.

However, Diebold is considering providing customers with information on how software products and services address PCI DSS requirements.

27. What merchant or service provider is eligible for a Self Assessment Questionnaire?

The SAQ is a validation tool for merchants and service providers who are not required to undergo an on-site data security assessment per the PCI DSS Security Audit Procedures. We recommended that merchants and service providers consult acquirers regarding validation requirements to determine if they are permitted to self-evaluate their PCI DSS compliance.

28. What ATM components are involved in PCI DSS assessment?

All ATM software components dealing with customers’ data are involved in a PCI DSS compliance assessment as none of them can violate PCI DSS requirements. This is the reason why Diebold has audited all software pieces running on Diebold ATMs and applied changes required to not violate applicable PCI DSS requirements.

29. Who is responsible for achieving ATM PCI DSS compliance?

The ATM software and services supplier is responsible for providing its customers with PCI DSS ready products and services for requirements that apply to ATM’s.

30. Who is responsible for achieving ATM PCI DSS assessment?

The ATM is a component of the bank network as defined by the cardholder data environment in the PCI DSS standard. The PCI DSS assessment of ATM’s is part of the overall assessment as required by acquirers for the bank. The assessor can verify whether ATM segmentation is adequate to reduce the scope of the PCI DSS assessment.

31. Who is responsible for achieving overall PCI DSS assessment?

PCI DSS compliance is expected for merchants and service providers that process, transmit or store cardholder data. Enforcement program may vary depending on the card acquirer (e.g. Self-Assessment, Qualified Security Assessor). It is recommended that merchants and service providers contact their acquirers for questions related to compliance validation requirements and deadlines.

32. What is a Qualified Security Assessor (QSA)?

A QSA is a data security company referenced by the PCI Council to perform on-site assessments for PCI DSS compliance and produce report on compliance (ROC). A list of QSAs is available on the PCI security standard web site:

https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

33. What is an Approved Scanning Vendor (ASV)?

An ASV is a data security company referenced by the PCI Council focusing on validating the compliance with the PCI DSS requirement related to external vulnerability scanning. A list of ASVs is available the PCI security standard web site:

https://www.pcisecuritystandards.org/pdfs/asv_report.html

34. What is a Self-Assessment Questionnaire (SAQ)?

An SAQ is a PCI DSS tool allowing merchants and service providers, who are not required to perform an on-site assessment, to perform a self-validation for PCI DSS compliance. There are five types of SAQ depending on the type of merchants.

Call on Diebold for the latest in product, service and security solutions.
Since 1859, Diebold has put the customer first.

Contact Information:
Diebold, Incorporated
5995 Mayfair Road
North Canton, Ohio 44720

E-mail: info@diebold.com
www.diebold.com

© Diebold, Incorporated, 2009. All rights reserved.
Litho in USA. File No. XX-XXX

