Payment Card Industry

Data Security Standard

Summary of Changes from PCI DSS Version 3.2.1 to 4.0

Revision 1

May 2022

Document Changes

Date	Revision	Description
March 2022		Initial release of the PCI DSS v3.2.1 to v4.0 Summary of Changes.
May 2022	1	Errata update to correct the change description for PCI DSS v4.0 Requirement 8.3.9.

Table of Contents

1 Introduction

This document provides a high-level summary and description of the changes from PCI DSS v3.2.1 to PCI DSS v4.0 and does not detail all document revisions. Due to the extent of the changes, the standard should be reviewed in its entirety rather than focusing solely on this summary document.

This Summary of Changes is organized as follows:

- *Change Types* - provides an overview of the types of changes
- *Summary of Changes to PCI DSS Introductory Sections* - summarizes changes made for each affected section.
- *Summary of General Changes to PCI DSS Requirements* - summarizes changes made throughout the requirements, testing procedures, and guidance.
- *Additional Changes per Requirement* - summarizes additional changes made in requirements 1-12 and the appendices.
- *Summary of New Requirements* - lists all new requirements, the entity to which the new requirement applies (that is, all entities or service providers only), and the effective date of the new requirement.

2 Change Types

Change Type	Definition
Evolving requirement	Changes to ensure that the standard is up to date with emerging threats and technologies, and changes in the payment industry. Examples include new or modified requirements or testing procedures, or the removal of a requirement.
Clarification or guidance	Updates to wording, explanation, definition, additional guidance, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Structure or format	Reorganization of content, including combining, separating, and renumbering of requirements to align content.

3 Summary of Changes to PCI DSS Introductory Sections

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Introduction and PCI Data Security Standard Overview	Introduction and PCI Data Security Standard Overview	Added “Limitations” sub-heading and clarified that PCI DSS does not supersede county, state, or local laws. Expanded list of PCI DSS resources.	Clarification or guidance
PCI DSS Applicability Information	PCI DSS Applicability Information	Added sub-headings to increase readability. Clarified that some PCI DSS requirements may apply for entities that do not store, process, or transmit primary account number (PAN). Clarified that terms account data, sensitive authentication data (SAD), cardholder data, and PAN are not interchangeable and are used intentionally in PCI DSS. Clarified table with commonly used elements of cardholder data and SAD, whether storage is permitted, and whether data must be rendered unreadable.	Clarification or guidance
Relationship between PCI DSS and PA-DSS	Relationship between PCI DSS and PCI SSC Software Standards	Refocused section on relationship between PCI DSS and PCI SSC software standards, with mention of PA-DSS (retiring in October 2022).	Evolving requirement
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements	Clarified applicability of PCI DSS requirements and the definition of cardholder data environment (CDE). Expanded examples of system components to which PCI DSS applies; added cloud and other system components. Added “Understanding PCI DSS Scoping” diagram.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements: Annual PCI DSS Scope Confirmation	Added sub-heading and clarified existing content.	Clarification or guidance
Appendix D: Segmentation and Sampling of Business Facilities/System Components	Scope of PCI DSS Requirements: Segmentation	Moved segmentation diagram formerly in Appendix D, with minor edits. Retitled sub-section and updated references from 'network segmentation' to 'segmentation' to support a broader range of segmentation controls.	Clarification or guidance
Scope of PCI DSS Requirements: Wireless	Scope of PCI DSS Requirements: Wireless	Clarified that rogue wireless detection (Requirement 11.2.1) must be performed even if wireless is not used in the CDE and even if the entity has a policy that prohibits its use.	Clarification or guidance
	Scope of PCI DSS Requirements: Encrypted Cardholder Data and Impact on PCI DSS Scope	Added sub-section and related content.	Clarification or guidance
	Scope of PCI DSS Requirements: Encrypted Cardholder Data and Impact to PCI DSS Scope for Third-Party Service Providers	Added new sub-section and related content.	Clarification or guidance
Scope of PCI DSS Requirements: Use of Third-party Service Providers/Outsourcing	Scope of PCI DSS Requirements: Use of Third-party Service Providers	Retitled sub-section, added new content, and reorganized existing content under new sub-headings.	Clarification or guidance
Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Added guidance and clarifications throughout.	Clarification or guidance
For Assessors: Sampling of Business Facilities/System Components	For Assessors: Sampling for PCI DSS Assessments	Retitled section and updated throughout with additional guidance and clarifications. Clarified that sampling references were removed from Testing Procedures to support assessors in selecting samples that are appropriate to the population being tested.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Appendix D: Segmentation and Sampling of Business Facilities/System Components	For Assessors: Sampling for PCI DSS Assessments	Moved sampling diagram formerly in Appendix D, with minor edits.	Clarification or guidance
	Description of Timeframes Used in PCI DSS Requirements	New section to clarify frequencies and timeframes specified in PCI DSS and related expectations. Added explanation of "significant change."	Clarification or guidance
	Approaches for Implementing and Validating PCI DSS	New section to explain and illustrate the two approaches, defined and customized, for implementing and validating PCI DSS.	Evolving requirement
Compensating Controls	Approaches for Implementing and Validating PCI DSS	Moved content to this section, at a sub-heading under "Defined Approach."	Structure or format
	Protecting Information About Entity's Security Posture	New section to describe how entities may handle sensitive artifacts from their PCI DSS assessment.	Clarification or guidance
	Testing Methods for PCI DSS Requirements	New section to describe the testing methods used in each PCI DSS Testing Procedures and corresponding expected activities to be performed by the assessor.	Clarification or guidance
PCI DSS Assessment Process	PCI DSS Assessment Process	Includes minor clarifications. Moved note that starts "PCI DSS requirements are not considered to be in place…" here, formerly in Detailed PCI DSS Requirements and Security Assessment Procedures.	Clarification or guidance
	Additional References	New section that lists external organizations referenced within PCI DSS requirements or guidance.	Clarification or guidance
Detailed PCI DSS Requirements and Security Assessment Procedures	Detailed PCI DSS Requirements and Testing Procedures	Replaced content on first page of section with an illustration that explains all elements of the Requirements column, Testing Procedures column, and Guidance column. To first page of section, added description for Requirements noted with "Additional requirements for service providers only." To first page of section, added summary of appendices that include additional PCI DSS requirements for different types of entities.	Clarification or guidance

4 Summary of General Changes to PCI DSS Requirements

General Changes Implemented Throughout PCI DSS Requirements	Change Type
Reformatted overview sections and added a summary of the sections to the beginning of each principal requirement.	Structure or format
Updated overview sections and added guidance at the start of each requirement section.	Clarification or guidance
Added numbered requirement description headings throughout each requirement to organize and describe the requirements that fall under it.	Structure or format
Renumbered requirements and testing procedures and reorganized requirements due to the addition of numbered requirement description headings.	Structure or format
Rephrased directive requirements to be objective.	Evolving requirement
Moved examples from requirements or testing procedures into the guidance column.	Structure or format
Removed references to sampling from testing procedures.	Clarification or guidance
Shortened testing procedures by clarifying testing is to be done “in accordance with all elements specified in this requirement” to minimize redundancy between requirements and testing procedures.	Clarification or guidance
Updated language in requirements and/or corresponding testing procedures for alignment and consistency.	Clarification or guidance
Enhanced testing procedures to clarify level of validation expected for each requirement.	Clarification or guidance
Reformatted requirements and testing procedures and made minor wording changes for readability – for example, content from paragraphs reformatted to bullet points.	Structure or format
Combined requirements that support the same intent and separated requirements that support different intents.	Structure or format
Separated complex requirements / testing procedures and removed redundant or overlapping testing procedures.	Structure or format
Moved required elements that were included only in testing procedures to requirements, to clarify the requirement and to facilitate shortening of the testing procedures.	Clarification or guidance
Moved and reworded policies and procedures requirements from the end to the beginning of each principal requirement.	Structure or format
Removed notes about SSL/Early TLS from the guidance columns for requirements that referenced those specific protocols.	Clarification or guidance
Changed “cardholder data” to “account data” as needed to align with usage and intent.	Clarification or guidance
Changed terminology used to refer to frequency throughout the requirements in accordance with Description of Timeframes Used in PCI DSS Requirements.	Clarification or guidance
Added titles and reorganized content of the guidance column to aid understanding and merge similar information.	Structure or format

5 Additional Changes per Requirement

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Requirement 1			
Requirement 1- General		Updated principal requirement title to reflect the focus on “network security controls.” Replaced “firewalls” and “routers” with “network security controls” to support a broader range of technologies used to meet the security objectives traditionally met by firewalls.	Evolving requirement
1.1.5	1.1.2	Replaced requirement for “Description of groups, roles, and responsibilities for management of network components” with general requirement for roles and responsibilities for Requirement 1.	Evolving requirement
1.1	1.2.1	Refocused former “null” requirement (all content pointed to other requirements) on defining, implementing, and maintaining configuration standards for network security control rulesets.	Clarification or guidance
1.1.1	1.2.2	Clarified that changes are managed in accordance with the change control process defined at Requirement 6.5.1.	Clarification or guidance
1.1.4		Removed redundant requirement.	Clarification or guidance
1.1.6	1.2.5 1.2.6	Separated into two requirements to clarify intent of each.	Clarification or guidance
1.1.7	1.2.7	Clarified the intent of reviewing configurations of network security controls at least once every six months.	Clarification or guidance
1.2		Removed “null” requirement (all content pointed to other requirements).	Structure or format
1.2.2	1.2.8	Clarified the intent of securing configuration files.	Clarification or guidance
1.2.1 1.3.4	1.3.1 1.3.2	Separated Requirement 1.2.1. into two requirements to clarify intent of each. Removed redundant Requirement 1.3.4.	Clarification or guidance
1.2.3	1.3.3	Clarified the intent of implementing network security controls between wireless networks and the CDE.	Clarification or guidance
1.3	1.4.1	Refocused a former null requirement (all content pointed to other requirements). Clarified that the intent is to implement controls between trusted and untrusted networks.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
1.3.1 1.3.2 1.3.5	1.4.2	Merged requirements to clarify that the intent is to restrict inbound traffic from untrusted networks.	Clarification or guidance
1.3.6	1.4.4	Clarified the intent is that system components storing cardholder data are not directly accessible from untrusted networks.	Clarification or guidance
1.4	1.5.1	Clarified that the intent is to implement security controls on any computing device that connects to both untrusted networks and the CDE.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Requirement 2			
Requirement 2 - General		Updated principal requirement title to reflect that the focus is on secure configurations in general, and not just on vendor-supplied defaults.	Clarification or guidance
	2.1.2	**New requirement** for roles and responsibilities. This requirement is effective immediately for all v4.0 assessments	Evolving requirement
2.1	2.2.2	Clarified that the intent is to understand whether vendor default accounts are in use and to manage them accordingly.	Clarification or guidance
2.2.1	2.2.3	Clarified the intent of the requirement for managing primary functions that require different security levels.	Clarification or guidance
2.2.2 2.2.5	2.2.4	Combined requirements to align similar topics.	Structure or format
2.2.3	2.2.5	Clarified that the intent of the requirement is if any insecure services, protocols, or daemons are present.	Clarification or guidance
2.1.1	2.3.1 2.3.2	Split requirement for changing all wireless vendor defaults into two requirements to clarify the focus of each.	Clarification or guidance
2.4	12.5.1	Moved requirement to align related content.	Structure or format
2.6		Removed “null” requirement (all content pointed to other requirements).	Structure or format
Requirement 3			
Requirement 3 - General		Updated principal requirement title to reflect the focus on account data.	Clarification or guidance
	3.1.2	**New requirement** for roles and responsibilities. This requirement is effective immediately for all v4.0 assessments.	Evolving requirement
3.1	3.2.1	**New requirement bullet** to address SAD stored prior to completion of authorization through implementation of data retention and disposal policies, procedures, and processes. This bullet is a best practice until 31 March 2025.	Evolving requirement
	3.3.2	**New requirement** to encrypt SAD that is stored electronically prior to completion of authorization. *This requirement is a best practice until 31 March 2025.*	Evolving requirement

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
3.2.a 3.2.b	3.3.3	Added a requirement to address former testing procedures that any storage of SAD by issuers is limited to that which is needed for a legitimate issuing business need and is secured.	Clarification or guidance
3.3	3.4.1	Clarified that PAN is masked when displayed such that only personnel with a business need can see more than the BIN/last four digits of the PAN.	Evolving requirement
12.3.10	3.4.2	**New requirement** for technical controls to prevent copy and/or relocation of PAN when using remote-access technologies. Expanded from former Requirement 12.3.10. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
3.4	3.5.1	Removed pads from the "Index tokens and pads" bullet for rendering PAN unreadable.	Evolving requirement
	3.5.1.1	**New requirement** for keyed cryptographic hashes when hashing is used to render PAN unreadable. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
	3.5.1.2	**New requirement** that disk-level or partition-level encryption is used only to render PAN unreadable on removable electronic media or, if used on non-removable electronic media, the PAN is also rendered unreadable via a mechanism that meets Requirement 3.5.1. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
3.5.1	3.6.1.1	**New requirement bullet for service providers only** to include in the documented description of the cryptographic architecture that use of the same cryptographic keys in production and test environments is prevented. *This bullet is a best practice until 31 March 2025.*	Evolving requirement

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Requirement 4			
Requirement 4 - General		Updated principal requirement title to reflect the focus on "strong cryptography" to protect transmissions of cardholder data.	Clarification or guidance
	4.1.2	**New requirement** for roles and responsibilities. *This requirement is effective immediately for all v4.0 assessments.*	Evolving requirement
4.1	4.2.1	**New requirement bullet** to confirm certificates used for PAN transmissions over open, public networks are valid and not expired or revoked. *This bullet is a best practice until 31 March 2025.*	Evolving requirement
	4.2.1.1	**New requirement** to maintain an inventory of trusted keys and certificates. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
Requirement 5			
Requirement 5 - General		Updated principal requirement title to reflect the focus on protecting all systems and networks from malicious software.	Clarification or guidance
		Replaced "anti-virus" with "anti-malware" throughout to support a broader range of technologies used to meet the security objectives traditionally met by anti-virus software.	Evolving requirement
	5.1.2	**New requirement** for roles and responsibilities. *This requirement is effective immediately for all v4.0 assessments.*	Evolving requirement
5.1.2	5.2.3	Clarified requirement by changing focus to "system components that are not at risk for malware."	Clarification or guidance
	5.2.3.1	**New requirement** to define the frequency of periodic evaluations of system components not at risk for malware in the entity's targeted risk analysis. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
5.2	5.3.1 5.3.2 5.3.4	Split one requirement into three to focus each requirement on one area: • Keeping the malware solution current via automatic updates, • Performing periodic scans and active or real-time scans (with a new option for continuous behavioral analysis), • Generation of audit logs by the malware solution.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
	5.3.2.1	**New requirement** to define the frequency of periodic malware scans in the entity's targeted risk analysis. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
	5.3.3	**New requirement** for a malware solution for removable electronic media. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
	5.4.1	**New requirement** to detect and protect personnel against phishing attacks. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
Requirement 6			
Requirement 6 - General		Updated principal requirement title to include "software" rather than "applications." Clarified that Requirement 6 applies to all system components, except for Requirement 6.2, which applies only to bespoke and custom software.	Clarification or guidance
	6.1.2	**New requirement** for roles and responsibilities. This requirement is effective immediately for all v4.0 assessments.	Evolving requirement
6.3	6.2.1	Moved requirement for developing software securely to align all software development content under Requirement 6.2.	Structure or format
		Replaced "internal and external" with "bespoke and custom" software. Clarified that this requirement applies to software developed for or by the entity for the entity's own use and does not apply to third-party software.	Clarification or guidance
6.5	6.2.2	Moved the elements of Requirement 6.5 for training of software developers to align all software development content under Requirement 6.2. Clarified training requirements for software development personnel.	Clarification or guidance
6.3.2	6.2.3 6.2.3.1	Moved requirement for reviewing custom software prior to release to align all software development content under Requirement 6.2. Split requirement to separate general code review practices from those needed if manual code reviews are performed.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
6.5.1 – 6.5.10	6.2.4	Moved requirements for addressing common coding vulnerabilities to align all software development content under Requirement 6.2. Combined methods to prevent or mitigate common software attacks into a single requirement and generalized the language describing each type of attack.	Clarification or guidance
6.1 6.2	6.3	Moved requirements for identifying security vulnerabilities and protecting system components from vulnerabilities via patching under Requirement 6.3.	Structure or format
6.1	6.3.1	Added a bullet to clarify applicability to vulnerabilities for bespoke and custom and third-party software.	Clarification or guidance
	6.3.2	**New requirement** to maintain an inventory of bespoke and custom software. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
6.6	6.4.1	Moved requirement for addressing new threats and vulnerabilities for public-facing web applications under Requirement 6.4.	Structure or format
	6.4.2	**New requirement** to deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks. This new requirement removes the option in Requirement 6.4.1 to review web applications via manual or automated application vulnerability assessment tools or methods. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
	6.4.3	**New requirement** for management of all payment page scripts that are loaded and executed in the consumer's browser. *This requirement is a best practice until 31 March 2025.*	Evolving requirement
6.3.1 6.4 6.4.1 – 6.4.6	6.5.1 – 6.5.6	Moved and combined requirements for changes to system components under Requirement 6.5.	Structure or format
6.4	6.5.3 6.5.4 6.5.5 6.5.6	Removed requirement for specific documented procedures and added testing procedures to verify policies and procedures to each related requirement.	Clarification or guidance
6.4.1	6.5.3	Changed term from "development/test and production" to "production and pre-production" environments.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
6.4.2	6.5.4	Changed term from “development/test and production” to “production and pre-production” environments. Changed term “separation of duties” and clarified that separation of roles and functions between production and pre-production is intended to provide accountability so that only approved changes are deployed.	Clarification or guidance
6.4.3	6.5.5	Changed term from “testing or development” to “pre-production” environments. Clarified that live PANs are not used in pre-production environments except where all applicable PCI DSS requirements are in place.	Clarification or guidance
Requirement 7			
Requirement 7 - General		Updated principal requirement title to include system components and cardholder data.	Clarification or guidance
	7.1.2	**New requirement** for roles and responsibilities. *This requirement is effective immediately for all v4.0 assessments.*	Evolving requirement
7.1	7.2.1 7.2.2 7.2.3	Removed requirement for specific documented procedures and added testing procedures to verify policies and procedures to each related requirement.	Clarification or guidance
7.1.1	7.2.1	Clarified requirement is about defining an access control model.	Clarification or guidance
7.1.2 7.1.3	7.2.2	Combined requirements for assigning access based on job classification and function, and least privileges.	Structure or format
7.1.4	7.2.3	Clarified requirement is about approval of required privileges by authorized personnel.	Clarification or guidance
	7.2.4	**New requirement** for review of all user accounts and related access privileges. This requirement is a best practice until 31 March 2025.	Evolving requirement
	7.2.5	**New requirement** for assignment and management of all application and system accounts and related access privileges. This requirement is a best practice until 31 March 2025.	Evolving requirement
	7.2.5.1	**New requirement** for review of all access by application and system accounts and related access privileges. This requirement is a best practice until 31 March 2025.	Evolving requirement

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
8.7	7.2.6	Moved requirement since it aligns better with the content in Requirement 7.	Structure or format
7.2		Removed "null" requirement (all content pointed to other requirements).	Structure or format
Requirement 8			
Requirement 8 - General		Standardized on terms "authentication factor" and "authentication credentials." Removed "non-consumer users" and clarified in the overview that requirements do not apply to accounts used by consumers (cardholders).	Clarification or guidance
		Removed note in overview that listed requirements that do not apply to user accounts with access to only one card number at a time to facilitate a single transaction and added that note to each related requirement.	Structure or format
	8.1.2	**New requirement** for roles and responsibilities. *This requirement is effective immediately for all v4.0 assessments.*	Evolving requirement
8.1.1	8.2.1	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Clarification or guidance
8.5	8.2.2	Changed focus of requirement to allow use of shared authentication credentials, but only on an exception basis.	Evolving requirement
		Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Clarification or guidance
8.5 8.5.1	8.2.2 8.2.3	Moved requirements for group, shared, or generic accounts and for service providers with remote access to customer premises under Requirement 8.2.	Structure or format
8.1.8	8.2.8	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Structure or format
8.2	8.3.1	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Structure or format

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
8.1.6 8.1.7	8.3.4	Merged requirements and moved under Requirement 8.3 Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Structure or format
		Increased the number of invalid authentication attempts before locking out a user ID from six to 10 attempts.	Evolving requirement
8.2.6	8.3.5	Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1.	Clarification or guidance
8.2.3	8.3.6	**New requirement** to increase password length from a minimum length of seven characters to minimum length of 12 characters (or if the system does not support 12 characters, a minimum length of eight characters). *This requirement is a best practice until 31 March 2025.* Clarified that, until 31 March 2025, passwords must be a minimum length of at least seven characters in accordance with v3.2.1 Requirement 8.2.3. Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1. Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Evolving requirement
8.2.5	8.3.7	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Structure or format
8.4	8.3.8	Moved content about communicating user authentication policies and procedures under Requirement 8.3.	Structure or format
8.2.4	8.3.9	Clarified that this requirement applies if passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation). Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. Added a note that this requirement does not apply to service providers' customer accounts, but does apply to accounts for service provider personnel.	Clarification or guidance