

## Data Security Standards for the Payment Card Industry and the Swivel Secure Solution

### What are the Standards and who do they apply to?

The Payment Card Industry (PCI) Data Security Standards (DSS) are comprehensive and have 12 different requirements within 6 different sections that cover the development and maintenance of a secure network to protect card holder data. The standards were developed by the founder members of the PCI Security Standards Council (SCC) which include the payment brands American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International. The standards apply to all organisations of all sizes working in the payment card industry including point of sale vendors, merchants, financial institutions and processors\*.

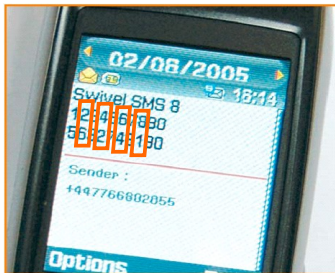


### Why should Businesses Comply?

The PCI SCC website states that "Security of payment account data is the responsibility of every business that participates in payment processing". Any business which does not adequately protect their account data is taking a risk. A breach of security may inevitably cost money. Whether through theft, prosecution, increased insurance costs or loss of reputation. Investment in compliance should not be avoided, it is not a luxury but a necessity to protect both customers and the business. Businesses are required to submit a compliance report to any payment brand that they accept and it is the payment brands which will enforce their own compliance programs. The threats to data security seem ever increasing and more sophisticated and more frequently highlighted in the media.

### What is Swivel Secure's Solution?

PINsafe, our award winning tokenless, two-factor authentication product is offered as a solution for Requirement 8 of the PCI Standard. This section of the standard relates to authentication and related access management.



PINsafe can be configured to send a Security String to a known user's mobile phone. The Security String, in conjunction with a PIN, creates a one-time code which is used as an authentication credential. The use of the mobile phone instead of a dedicated security token makes deployment much more straightforward and there are no on-running token management costs.

### Key Elements on PINsafe in relation to PCI Section 8

Section 8 has a number of requirements relating to authentication and user identification. These are summarised below with insight into how PINsafe can help meet those requirements.

[www.ansecurity.com](http://www.ansecurity.com) 0845 226 0462



## Protection in a Hostile World



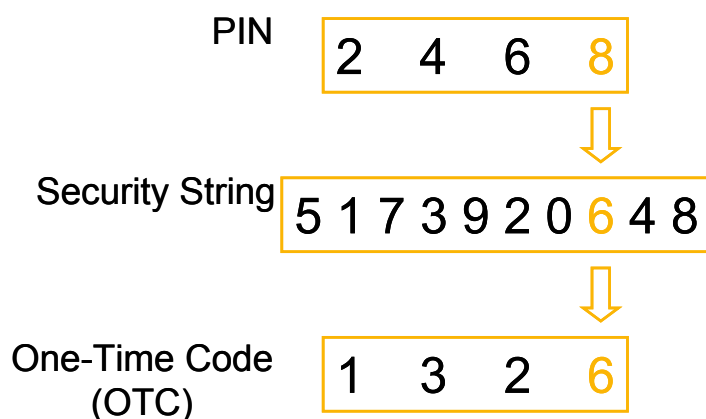
## Authentication

PCI requires strong authentication and specifically two-factor authentication for remote access. PINsafe utilises the user mobile phone as a factor of authentication; without access to the specific mobile phone a user cannot authenticate. As the user already has a mobile phone there is no need for an additional authentication token. Also, as the mobile phone has become such an integral part of our lives, users are more likely to notice and report the loss/theft of their mobile phone than they are a dedicated authentication token.

PINsafe is easy to deploy as part of a remote access solution. PINsafe incorporates a RADIUS server that can be used to integrate with a vast range of SSL VPN solutions, providing the best user experience. This includes the ability, in certain circumstances, to provide single stage PINsafe and domain authentication.

## Credentials Management

PCI requires that a user's authentication credentials change on a regular basis. The PINsafe protocol sends a different security string to the user everytime they authenticate, meaning PINsafe adheres to the PCI directive.



In addition on PINsafe you can set policies to ensure that users change their PIN on a regular basis and/or change it at their first log-in.

PINsafe allows a user to set their own PIN; when a PIN change is required the new PIN must be different to the existing PIN. PINsafe policies can be set to prevent users changing their PINs to 1234 or 0000 etc.

## User Management

PCI requires that access only be granted to authorised users with sufficient rights and that access can be revoked in a timely manner. It also calls for users to be disabled after prolonged non-usage.

All these elements are covered by PINsafe. PINsafe can be integrated with an enterprise's exist user-management system, eg Active Directory. Therefore creating a new PINsafe account requires a new AD account, something only an administrator can do. Similarly if the account is disabled or removed from AD the corresponding action will be performed within PINsafe.

PINsafe can be configured to disable users who have not accessed the system for a specified length of time, in addition to locking out accounts that have had a specified number of failed authentication attempts.

## Summary

Ease of integration, no need to deploy a physical token combined with strong mobile-based two factor authentication means that PINsafe provides a painless way to contribute to meeting PCI requirement.

For **contacts** and further **information** about PINsafe and Swivel Secure Ltd visit our website on [www.swivelsecure.com](http://www.swivelsecure.com)

\*Source:<https://www.pcisecuritystandards.org/about/faqs.htm#q2>

