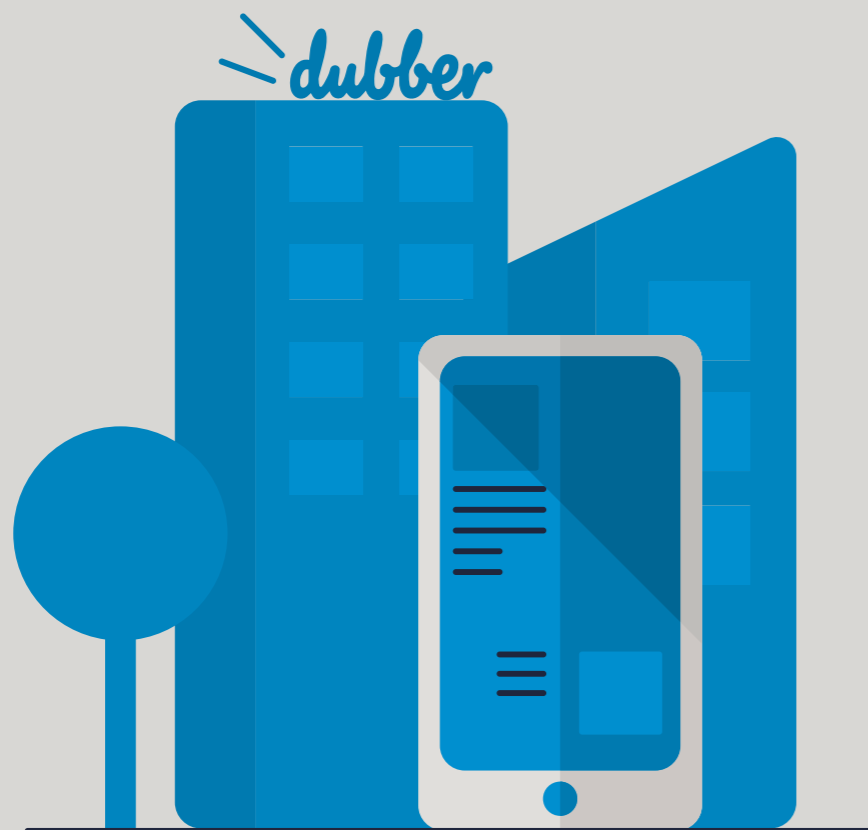


Call Recording for Payment Card Industry (PCI) White Paper



Contents

01 What is PCI DSS

- 01.1 History
- 01.2 PCI DSS Overview
- 01.3 PCI DSS Requirements for Call Recording

02 PCI DSS Requirements Breakdown

- 02.1 Build and maintain a secure network
- 02.2 Protect cardholder data
- 02.3 Maintain a vulnerability management programme
- 02.4 Implement strong access control measures
- 02.5 Regularly monitor and test networks
- 02.6 Maintain an information security policy

03 Dubber Call Recording & PCI Compliance

- 03.1 Automated Pause/Resume
- 03.2 Automation Methods
- 03.3 API
- 03.4 PCI Payment Node

04 Additional Dubber PCI Security Features

05 The Dubber Fulfilment of PCI DSS Requirements

- 05.1 Build and maintain a secure network
- 05.2 Protect cardholder data
- 05.3 Maintain a vulnerability management programme
- 05.4 Implement strong access control measures
- 05.5 Regularly monitor and test networks
- 05.6 Maintain an information security policy

06 About Dubber

01 What is PCI DSS

The total number of payment card transactions throughout the world in 2015 was over 400 billion and by 2020, is expected to grow to around 750 billion. With identity theft and organised card crime prevalent within today's society, the requirement for secure transactions is more critical than ever.

01.1 History

In 2001, VISA mandated the Cardholder Information Security Program (CISP). VISA provided this initiative specifically for merchants and service providers who processed, stored or transmitted cardholder data. The initiative's goal was to ensure that cardholders' account details would be made secure protecting the customer.

Following VISA's initiative, other card providers started similar programmes to provide security to their customers, these included MasterCard's Site Data Protection (SDP) and American Express' Data Security Operating Policy. These policies ensured that any merchant would be mandated to provide a level of protection for card issuers by ensuring that merchants met levels of security when they store, process and transmit cardholder data.

In 2004, the major card companies aligned to form the Payment Card Industry Security Standards Council (PCI DSS). On December 15th 2004, the PCI DSS 1.0 was released.

Over the following years PCI DSS has evolved to not only provide greater security to the industry, but also to accommodate new technology advancements and is today the global data security standard for payment cards.

01.2 PCI DSS Overview

PCI DSS details security requirements for members, merchants and service providers that store, process or transmit cardholder data. PCI regulations forbid storing primary account numbers (PAN), expiration dates, and other specified identifiers unless they meet PCI-DSS encryption standards. In addition, security codes and PIN numbers must not be stored even if encrypted.

It is the merchant that required PCI DSS compliance and certification. The aim of the systems vendors is to provide the tools with which to enable the merchant to attain PCI DSS.

Depending upon the amount of transactions being processed, the merchant may be either complete a self-assessment questionnaire (if they complete less than 300,000 transactions annually) or require on site inspection to become PCI DSS if the number of transactions is over 300,000 per annum. In order to complete the PCI DSS certification, all elements of the control objectives and requirements must be met.

01.3 PCI DSS Requirements for Call Recording

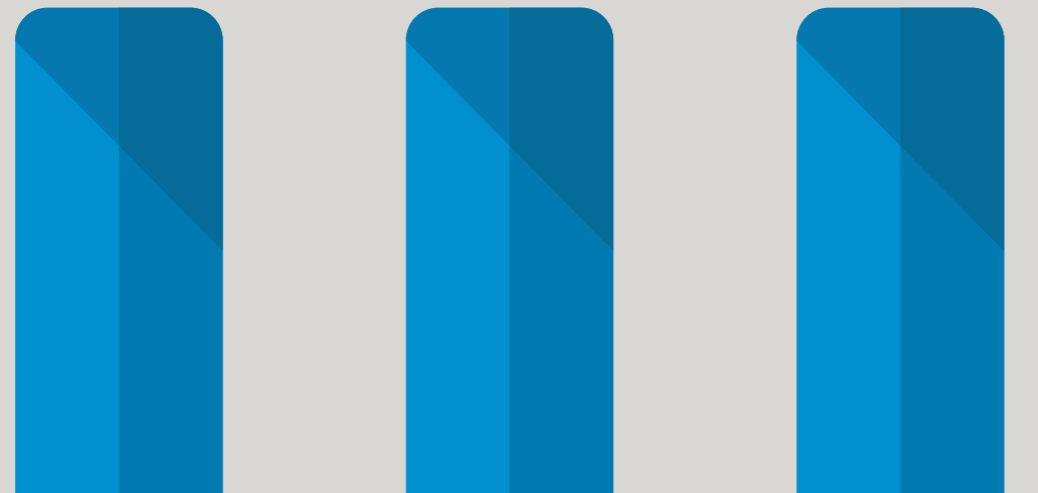
While PCI DSS is primarily aimed at cardholder information in databases, contact centres are presented a different set of complexities for both the agent handling the call and also the recording of the call.

In order to ensure that restricted information is not held within a call recording, numerous technologies have been used including:

- Manual Pause and Resume
- Automated Pause and Resume based on
- Desktop Activity
- Post call processing to remove credit card details from complete recordings
- IVR based DTMF payment systems



02 PCI DSS Requirements Breakdown



PCI DSS provides a framework to ensure compliance through a series of 'Control Objectives'. In order to comply with these PCI DSS Control Objectives, individual PCI DSS requirements must be adhered to.

The Control Objectives are separated into 6 sections covering all relevant control over environments that handle card payments. The list below outlines the current Control Objectives and PCI DSS requirements:

02.1 Build and maintain a secure network:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

02.2 Protect cardholder data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

02.3 Maintain a vulnerability management program

5. Use and regularly update anti-virus software on all systems commonly affected by malware
6. Develop and maintain secure systems and applications

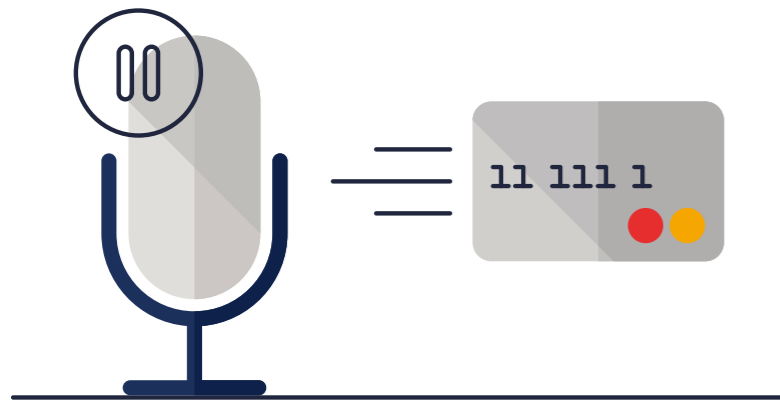
02.4 Implement strong access control measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

02.5 Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data
 11. Regularly test security systems and processes
- Maintain an information security policy
12. Maintain a policy that addresses information security

03 Dubber Call Recording & PCI Compliance



Dubber provides telephony users with all the tools necessary to achieve full PCI compliance. With the ever changing landscape of PCI DSS, new requirements are being demanded at each turn. Dubber is constantly working to ensure the tools required for PCI DSS are delivered to our users through on going development and feature enhancements.

Dubber currently supports the following tools, enabling end users to manage their PCI DSS requirements:

03.1 Automated Pause/Resume

Dubber's PCI integration technology with Automated Pause/Resume helps customers to comply with the Payment Card Industry's Data Security Standard (PCI DSS). This is accomplished

by automatically muting and unmuting a recording when pre-defined system events are detected. This can be achieved by one of the following options:

- Desktop and Browser: A client program is installed on the end user's PC which will detect window or URL changes and issue mute and unmute messages based on these changes
- Dubber API: The customer's payment program is modified to send mute and based on these changes unmute messages to the BroadWorks via a Dubber API installed on the Dubber record server

03.2 Automation Methods

The Dubber Automated Pause/Resume is provided in 2 different methods:



Desktop Client

- Low cost off-the shelf solution
- No customer development required
- Additional CRM / DB integrations available
- Simple workflow can be managed to enable pause and resume based on simple changes in URL etc.

03.3 API

- Mute / Unmute message closely integrated to end-user PCI solution
- More robust and less sensitive to end-user interference
- API allows advanced custom development for customer applications ensuring that any application can be used to trigger pause / resume messaging

03.4 PCI Payment Node

		
Trusted Thousands of transactions rely on the Dubber Payment Node.	Compliant Recording No payment details will be recorded via PCI Payment Node.	DTMF Suppression Agents are removed from the call and hear no DTMF tones.

The Dubber PCI Payment Node can easily implement PCI compliant payments using the new Dubber PCI Payment Node. The PCI Payment Node allows users to specify all the prompts and call logic necessary to take credit card payments. By combining the PCI Payment Node into the call flow, Dubber enables payments to different merchants depending on what payment processor is chosen by the client.

The different requirements of the various payment processors are all encapsulated within the Payment Node Profile Controller. There is no limit to the number of Merchant profiles.

The Payment Node ensures that PCI logging is handled appropriately. Restricted information such as Credit Card number, CVW number and Expiry Date are prevented for being used elsewhere within the tool and all logging is fully PCI compliant. All necessary audit logs required for compliance within the PCI process are automatically captured and preserved by the platform.

Agent Triggered Payments Process

During a call, a PCI compliance transaction is required and the process is triggered by agent. At that point the agent transfers call to the PCI Payment Node (hotkey or phone number) the Node scripts take over, requesting the relevant details (e.g. amount, card number etc). The captured payment details are sent automatically to the merchant for completion. Once the transaction is completed, the caller is connected back with the agent to complete the call.

During the transfer to the PCI Payment Node, the agent is not included in the call. This ensures that there is no chance of the payment details being captured in the recorded call or DTMF tones being heard by the agent.

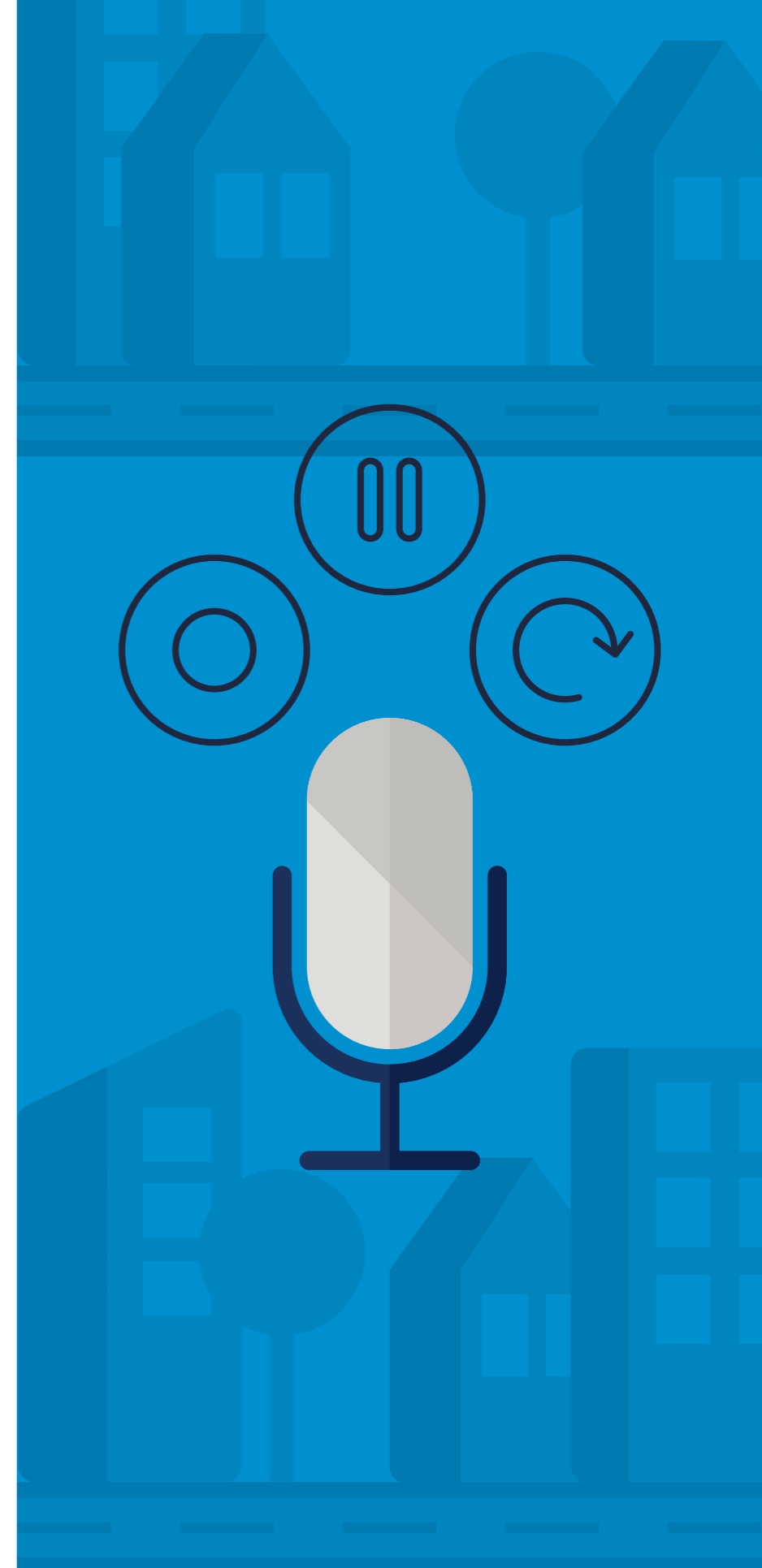
Additional benefits are also available with the PCI Payment Node that can enable functionality through both Self Service IVR payment management and can also assist outbound collections operations by automatic payment collection.

04 Additional Dubber PCI Security Features



Use of the Dubber Automated Pause and Resume and the Dubber PCI Payment Node effectively ensures PCI DSS compliance with regards to storage of sensitive data. As the initial recording has been made these 2 methods actively remove the sensitive data from the recording, either through an automated pause and resume or by relaying the caller to the Payment IVR during which time there is no active recording. In order to ensure full compliance in the event that payment card details are captured through failure of user processes, Dubber also enables users to ensure that the systems storing this data will meet compliance approval through additional security features within the platform as listed below:

- Media File Encryption - All recordings within the Dubber platform are encrypted as per PCI DSS guidelines
- Secure access to the recordings – Access to recordings is only available to valid and authenticated users with correct permissions
- All accounts within Dubber are subject to tenancy restrictions
- Secure access to the web portal via SSL (https access).
- Download/Export permissions are only available to specific user types enabling additional restricted access to recordings
- Authentication Rules for all users as per PCI DSS guidelines – including password complexity and lock out methodology
- Token based session security on all access to the Dubber Portal
- Automated Screening / Removal – Dubber is also able to remove sensitive information from recordings through our post processing biometric engine. This process removes any credit card data contained within the recording
- Complete Audit Trail – Dubber provides a full audit trail of all transactions within the platform, including write, read, search, playback, share and download



05 The Dubber Fulfilment of PCI DSS Requirements



05.1 Build and maintain a secure network

1. Install and maintain a firewall configuration to protect cardholder data

This item is primarily related to the customer network, but as Dubber is a SaaS platform, to ensure that the end customer has additional security, Dubber provides security across all components of the platform with secure transmission of recordings both to and from the recorders and platform.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Dubber does not provide any default passwords within the platform. All passwords are end user set and can be managed by the user directly. Passwords relate directly to the user and their dedicated User ID and email address, ensuring two-factor authentication during account creation and password selection.

05.2 Protect cardholder data

3. Protect stored cardholder data

Providing Automated Pause and Resume or PCI Payment Node have been used there should be no PCI sensitive data stored on the platform. In the event that data may be stored for parties with a waiver from PCI DSS (having a business need to store sensitive data) Dubber enables complete management of recordings through the Dubber Platform. End Users are able to fully manage recordings within Dubber based on their user type and access permissions.

Dubber also provides various levels of encryption across the entire platform including recordings and associated metadata.

Access to recordings within Dubber is only available to the end user, Dubber has no access to the recordings within the platform as the encrypted files are only accessible through the Dubber Platform to authenticated users with the appropriate permissions.

4. Encrypt transmission of cardholder data across open, public networks

The Dubber Recorder connects to the service provider telephony platform through a dedicated network connection. It should also be noted that providing the Automated Pause and Resume or PCI Payment Node is being utilized the audio traffic from the service provider should not contain any PCI DSS related data in the first instance.

05.3 Maintain a vulnerability management programme

5. Use and regularly update anti-virus software on all systems commonly affected by malware

As a 'native cloud' application, Dubber has been architected to

meet the highest security standards. All system components are constantly monitored to ensure there are no threats to both the system and any data stored within Dubber. Files within Dubber are created directly by the platform and all methods of ingress require full user authentication and are highly secure.

Dubber utilises scalable real time Antimalware and Antivirus protection across file systems, memory, processes and registry databases. These tools are seamlessly integrated into the Dubber Management Layer offering Dubber total security of all components within the Dubber system.

6. Develop and maintain secure systems and applications

Dubber ensures the security of the platform by developing and managing the systems through internal dedicated bespoke tools. Primary focus of the Dubber development and security teams is to ensure they manage features and functionality whilst providing the highest standard of security to the end users as possible.

05.4 Implement strong access control measures

7. Restrict access to cardholder data by business need-to-know

The Dubber platform should not contain any cardholder data providing the user has utilised any tools available to them to prevent recording of the cardholder data.

In the event that cardholder data is captured within Dubber, all access to Dubber and data contained within is controlled by advanced password and user authentication and additional security policies that enable system administrators to restrict access to recordings at the user level. This enables end users full control of both the environment and the users within that environment.

8. Assign a unique ID to each person with computer access

Dubber provides tokenised access to the portal to authenticated users. Each user that has access to Dubber is provided with unique username and password credentials. Additional security is also applied to ensure verification of authorized users.

9. Restrict physical access to cardholder data

Cardholder data that may be stored within Dubber is stored in the some of the most secure data centres in the world. Data is inaccessible through any method other than by authenticate users with the correct credentials. Access to the physical data would be virtually impossible as the storage arrays containing the data are dynamic and may be held in multiple data centres within a single geographic region at any point in time.

05.5 Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data

Dubber provides total audit trail for all recordings within the platform. Audit trail data is contained for all search and read activity. Dubber captures data on the transaction and the user requesting the data.

11. Regularly test security systems and processes

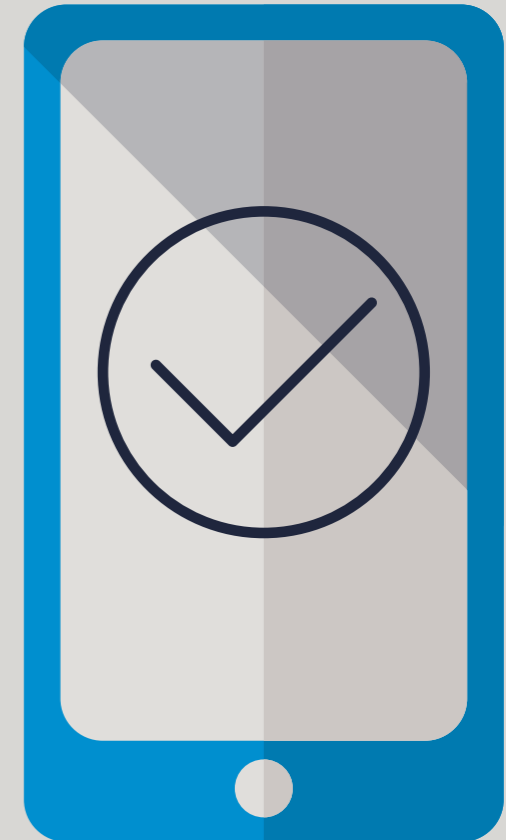
To ensure the security within the platform, Dubber undergoes regular penetration tests to ensure reliability throughout the platform. All elements of the Dubber platform are tested including tests run by the external security team within the actual Dubber platform.

As part of this penetration testing advance planning is completed to ensure that as the frameworks that Dubber is built upon, future security is taken into consideration.

05.6 Maintain an information security policy

12. Maintain a policy that addresses information security

Remember, PCI DSS requires the end user to be compliant, not the systems they are using. Most important to PCI DSS, is the fact that the end user is responsible for their own compliance. Dubber is able to provide some of the tools to enable PCI DSS compliance, but ultimately security of the end users card data and the policies surrounding this information security is the domain of the end user.



About Dubber

Dubber is the world's most scalable call recording service which enables service providers and customers to think about capturing voice data in a way which they have never previously considered. A true native cloud platform, Dubber is revolutionising the call recording industry. Its high availability, unique total scale and true Software as a Service (SaaS) offering enable telecommunications carriers and customers to implement and manage recordings as never before without the need for hardware or capital expenditure.



Get in touch

media 9
connected cloud solutions

01908 915065

media9.co.uk

admin@media9.co.uk



Copyright © 2016, Dubber. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. Dubber specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.