PLACE GROUP UK

LONDON STUDENT HOUSING GROUP

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD COMPLIANCE STATEMENT PCI DSS (09)

VERSION: 2009PCIDSSP4S01

Information updated: 21 October 2012

SAFEGUARDING CARDHOLDER DATA IS A LEGAL REQUIREMENT

WHY RISK YOUR CARD DETAILS WITH A BUSINESS OR LANDLORD WHO IGNORES COMPLIANCE ?

PLACE GROUP PAYMENT PROCESSING SYSTEMS HAVE BEEN CERTIFIED TO COMPLY WITH PCI DSS BY TRUSTWAVE.

CLICK HERE TO VIEW OUR COMPLIANCE CERTIFICATE

CLICK HERE FOR MORE GENERAL INFORMATION

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) comprises a set of comprehensive requirements, developed by MasterCard and Visa which set out requirements intended to safeguard cardholder data. Businesses accepting credit or debit cards must therefore ensure (either directly and/or through their third party processing agents) that the following requirements are met :

Build and Maintain a Secure Network

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

THE PLACE GROUP CARDHOLDER SECURITY POLICY :

At place group we understand what data elements the PCI DSS do permit businesses to store and that measures must be taken to protect those data, if stored. We also recognise that it is best practice for businesses NOT to store ANY cardholder data. Our cardholder security policy is based around this practice.

Our policy comprises four key staff knowledge elements, the fourth of which is the in house "Do and Don't" rules, and an additional fifth element, our "third party processing" guidelines.

1. All staff have a clear definition of cardholder data :

Information contained on a client's payment card (credit or debit card) is defined as "cardholder data". In general, cardholder data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the back side of the card and in chips embedded on the front side. In addition the front side usually has the primary account number (PAN), cardholder name and expiration date. The magnetic stripe or chip holds these plus other sensitive data for authentication and authorization.

2. All staff have a clear definition of what elements of cardholder data the PCI DSS do permit business to store and what elements businesses are prohibited from storing:

The PCI DSS state that cardholder data should never be stored unless it's necessary to meet the needs of the business and that sensitive cardholder data on the magnetic stripe or chip must never be stored. Only the PAN, expiration date, service code, or cardholder name may be stored, and with precautions for safe storage.

3. All staff understand the difference between collection and storage of cardholder data and how this impacts on how cardholder data is processed and our own procedures:

Whilst it may be necessary for us to collect cardholder data for processing purposes (for example collecting a PAN number from a client for telephone processing) all staff know that this cardholder data should not then be stored after processing. Staff understand why we ask clients either to request an electronic invoice by email so they can make payment directly through our third party processors, or for clients to provide payment card details by telephone which are entered in real time into the processing terminal. All staff understand that payment card details provided by telephone must be entered in real time direct to the processing terminal and not stored for later processing. Equally, staff understand why we ask client's not to email payment card details to us as this form of communication is insecure and the email may amount to a form of storage on our server or may be intercepted during transmission.

4. All staff know the place group own in house rules (the " DO and DONT rules") for cardholder data security:

We DO :

understand where cardholder data flows for the entire transaction process

verify that payment card terminals comply with the personal identification number entry device (PED) security requirements

verify that payment applications comply with the Payment Application Data Security Standard (PA-DSS)

ensure that the third parties who process our clients' payment cards themselves fully comply with PCI DSS, PED and/or PA-DSS as applicable

have clear access and password protection policies

We DO NOT :

(after processing and authorization (or refusal) of the payment card) store in any format or media, any cardholder data specifically but not limited to credit or debit card (or other payment card) numbers (the long PAN number across the front of the payment card), the printed 3-4 digit card validation code on the front or back of the payment card, nor any valid from or expiry dates, nor the sensitive authentication data contained in the

payment card's storage chip or full magnetic stripe. In particular, we do not store any cardholder data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones

have PED terminals which print out cardholder data or other personally identifiable payment card data

permit any unauthorized (or untrained) people to access cardholder data at any stage during the processing

5. We implement and monitor the Payment Application DSS Requirements (PA-DSS) which third parties who process place group clients' payment cards must comply with (our "third party processing" guidelines:

We recognize that whilst outsourcing simplifies payment card processing, it does not provide automatic compliance. We still protect cardholder data when we receive it and crucially also ensure that our providers' applications and card payment terminals comply with respective PCI standards and do not store sensitive cardholder data.

Therefore we require that our third party providers:

1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CIV2, CW2) or PIN block data

2. Provide secure password features

3. Protect stored cardholder data

4. Log application activity

5. Develop secure applications

6. Protect wireless transmissions access

7. Test applications to address vulnerabilities

8. Facilitate secure network implementation

9. Do not store cardholder data on a server connected to the Internet

10. Facilitate secure remote software updates

11. Facilitate secure remote access to application

12. Encrypt sensitive traffic over public networks

13. Encrypt all non-console administrative access

14. Maintain instructional documentation and training programs for customers, resellers and integrators