September 2015

LLOYDS BANK

CARDNET

Helping you meet your compliance obligations and changes to your terms and conditions

Dear Customer

All businesses that process card payments need to be fully compliant with the Payment Card Industry Data Security Standards (PCI DSS) and to validate their compliance each year. These Standards set by Card Schemes including Visa and MasterCard are in place to keep cardholder data safe, by making sure all card transactions are processed, transmitted and stored securely.

So that you meet these PCI DSS requirements and avoid non-compliance charges, we want to remind you of your PCI DSS obligations and let you know about the options that you have to validate your compliance. We also need to inform you of changes we are making to your Retailer Agreement and Operating Manual which will take effect on **31 October 2015**.

CMS300 (10/15)

The steps to become PCI DSS compliant

To be compliant you need to complete a PCI DSS Self Assessment Questionnaire (SAQ) which is a self validation tool. If you don't do this, you may face financial penalties and/or withdrawal of your card acceptance facility. The options you have to complete your SAQ are:

- You can self-certify through the PCI Security Standards Council for free at **pcisecuritystandards.org** or use a third party provider to become compliant. Once compliant you will need to upload your compliant SAQ or third party certificate onto our online PCI DSS portal, at no charge.
- You can manage your compliance through our fully managed PCI DSS portal. This managed solution helps you to understand which requirements are appropriate and guides you through your SAQ, providing support at every stage. There is a monthly fee for this service, which is currently £5.50 per outlet. We will be mailing you further information and login details for the portal within the next six weeks.

I have included more information on these options and PCI DSS in the enclosed Data Security fact sheet.

Whichever option you choose to achieve compliance you will need to access our PCI DSS portal. We will send you your login details for this within the next six weeks, along with a reminder about your options. You will then have three months to confirm your compliance through the portal. If you don't do this, we will charge you a non-compliance charge until you confirm your compliance. This non-compliance charge is currently £20.00 per month, per outlet.

If you have any questions about PCI DSS compliance, please call our PCI helpline on **0330 8080798.** Lines are open from 9am to 5pm, Monday to Friday.

Continued overleaf

Updates to your terms and conditions

We are also making changes to your Retailer Agreement and Operating Manual for PCI DSS, and these will take effect from the **31 October 2015**. As part of these changes, we are also removing the Data Security liability waiver for all businesses. This means that we will no longer cover the first £50,000 of expenses for a Data Security Event.

I have included more details about the changes with this letter – please read this carefully. I have also enclosed your new Retailer Agreement and you can find your new Operating Manual at **lloydsbankcardnet.com/operatingManual**

Our Agreement allows us to make a change to your terms and conditions by giving you 30 days notice. If you accept these changes there is nothing you need to do. But, if you are not happy with them, please call us on **01268 567 100**. Lines are open from 9am to 5pm, Monday to Friday.

Yours sincerely

Aidene Walsh
Commercial Cards Director

Changes to your Retailer Agreement from 31 October 2015

Section of the Retailer Agreement that is being updated:	Summary of the Change	The Change
Part 1 Clause 1 – Definitions and Interpretation	The definition of Data Security Event has been added to this section.	The following new definition is included: **Data Security Event** means any event where Cardholder data or Transaction Data (including any Card data or personal data) is stolen, misused or disclosed to any unauthorised person.
Part 1 Clause 16 – Data Security	You must comply with PCI DSS at all times, and validate your compliance with us annually. If you have a data security breach, you will be liable for any costs associated with that breach. We will no longer cover the first £50,000 of expenses. This applies to both compliant and non-compliant customers.	Clause 16.1 is amended to include an obligation to comply with PCI DSS at all times and to validate such compliance on an annual basis. Clause 16.2 is amended to reflect the new definition of Data Security Event. Clauses 16.8 and 16.10 (waiver by the Bank to recover from the Retailer the first £50,000 of expenses in connection with a Data Security Event) are deleted and replaced with the following: Clause 16.8 The Retailer shall indemnify and hold harmless on demand and on an after tax basis the Bank from any and all claims, proceedings, actions, complaints, fines, liabilities, penalties or demands from third parties (including without limitation Cardholders, Card Schemes, Payment Service Providers or the PCI SSC) and any losses, damages, costs or expenses directly or indirectly arising out of or in connection with any Data Security Event in full.
Part 1 Clause 19 – Sums Payable by the Retailer	If you chose to validate your compliance through our PCI DSS Portal, we will charge you a monthly management fee as set out in your Special Conditions. This is currently £5.50 per month, per outlet. If you chose to validate your compliance by completing a Self Assessment Questionnaire (SAQ) through the PCI Security Standards Council (SSC) website at **pcisecuritystandards.org** or through another third party provider, that monthly management fee will not be charged to you. You will need to upload a valid SAQ or third party certificate to the PCI DSS portal within three months from receiving your portal login details. After this three month period you will be charged a non-compliance charge for each month you remain non-compliant. This is currently £20 and is charged per month, per outlet. This charge of £20 was previously added on top of the management fee.	Clauses 19.1.11 and 19.1.12 are amended as follows: 19.1.11 if the Retailer validates PCI DSS compliance using the PCI DSS Portal, a monthly management fee as set out in the Special Conditions (the "PCI DSS Management Fee") will be applied three months after receipt by the Retailer of a letter from the Bank providing the initial password for access to the PCI DSS Portal. For the avoidance of doubt, if the Retailer validates its compliance with PCI DSS by completing a Self Assessment Questionnaire (SAQ) via the PCI SSC website (**pcisecuritystandards.org**) or through another third party provider, the PCI DSS Management Fee shall not be applied, provided that the merchant uploads a valid SAQ or third party certificate to the PCI DSS Portal within three months of receipt by the Retailer of a letter from the Bank providing the initial password for access to the PCI DSS Portal; 19.1.12 a monthly non-compliance charge as set out in the Special Conditions (the "PCI DSS Non-Compliance Charge") if (i) the Bank determines that the Retailer has failed to complete the annual PCI DSS validation process and upload its compliant SAQ or third party certificate to the PCI DSS Portal within three months of receipt by the Retailer of a letter from the Bank providing the initial password for access to the PCI DSS Portal, or (ii) the Retailer has failed to complete the annual PCI DSS validation process to indicate that its compliance has been renewed within 3 months of the relevant renewal date. For the avoidance of doubt, the PCI DSS Non-Compliance Charge shall be payable instead of the PCI DSS Management Fee. The PCI DSS Non-Compliance Charge shall be payable by the Retailer for each month that it is non-compliant until such time as the Retailer has validated its compliance by uploading its compliant SAQ or third party certificate to the PCI DSS Portal and completed the annual PCI DSS validation process. For those retailers who entered into agreements with us before September 2013, the Inactivity Fee referred to in clause 19.1.12 is deleted.
Part 1 Clause 32 – Termination	If you fail to validate your PCI DSS compliance, we have the right to terminate your Agreement with us.	A new clause 32.2.2.9 is added to allow the Bank to terminate the Agreement at any time forthwith in the event that the Retailer fails to validate its compliance with PCI DSS in accordance with Clause 16.1.

You can find your new updated versions at **lloydsbankcardnet.com/termsandconditions**

Our service promise

We aim to provide the highest level of customer service possible. However, if you experience a problem, we will always seek to resolve this as quickly and efficiently as possible. A copy of our 'How to complain' leaflet can be obtained by contacting the Cardnet Helpline on **01268 567100** or at **lloydsbankcardnet.com/how-to-complain**

Please contact us if you'd like this in an alternative format such as Braille, large print or audio.

Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service.

PCI_DSS_LTR2 (09/15)

LLOYDS BANK

CARDNET

Payment Card Industry Data Security Standards (PCI DSS)

What are the Payment Card Industry Data Security Standards	The Payment Card Industry Data Security Standards (PCI DSS) are the global rules that all businesses that process card payments need to be fully compliant with. PCI DSS compliance is mandated by the Card Schemes, including Visa and MasterCard, and relates to the secure transmission, receipt, and storage of cardholder data. These Standards are in place to keep cardholder data safe, by making sure all card transactions are processed, transmitted and stored securely.
How it applies to you	All businesses that process credit or debit card payments need to be fully compliant with PCI DSS and to validate their compliance each year. There are twelve PCI DSS requirements that you need to review. Some or all may be applicable to you dependant on your type of business and if you store card data.
What you need to do	To understand which of these requirements relate to you, and to validate your compliance, you need to complete a PCI DSS Self Assessment Questionnaire (SAQ).
Your options to complete your PCI DSS compliance obligations	You can complete a SAQ and validate your PCI DSS compliance in a number of ways: ▪ compliance through us by using our online PCI DSS portal for a monthly management fee, currently £5.50 per outlet ▪ compliance through a third party provider ▪ self-certify for free. You can take this option even if you are currently using our PCI DSS portal. **Compliance through us** You can use our upgraded online PCI DSS portal which you can fi nd at **lloydsbankcardnetpcidss.com** There is a monthly fee to use this service, this is currently £5.50, per outlet. Our PCI DSS portal includes: ▪ an easy to use online tool that helps you through the Self Assessment Questionnaire, supporting you at each stage to help you understand and meet your validation requirements ▪ a dedicated helpline that is available to support you with any questions relating to PCI DSS compliance you may have ▪ access to a Qualified Security Assessor (QSA) for more complex technical information and guidance, where needed ▪ if you have a Point of Sale device with an internet connection and are accepting card-not-present cardholder payments through a virtual terminal or you're a business hosting their own e-commerce payment pages, we have unlimited network vulnerability scanning of 1 IP address. **Compliance through a third party provider** ▪ You can validate your compliance through a third party provider by selecting a Qualified Security Assessor (QSA) on the PCI Security Standards Council (SSC) website at **pcisecuritystandards.org/approved_companies_providers/qsa_companies.php** ▪ You will need to confirm your compliance by uploading your Self Assessment Questionnaire (SAQ) or third party certificate, at no charge, to **lloydsbankcardnetpcidss.com** **Self-certifying your compliance** ▪ To self-certify, visit the PCI Security Standards Council website at **pcisecuritystandards.org** and complete your own Self Assessment Questionnaire (SAQ). ▪ You will need to confirm your compliance by uploading your Self Assessment Questionnaire (SAQ), at no charge, to **lloydsbankcardnetpcidss.com**

How to access our PCI DSS portal	You will receive your login details by post within six weeks. When you have received your login details, visit **lloydsbankcardnetpcidss.com** to access the portal. If you haven't received anything by 1 December 2015, please contact us on **0330 808 0798.** Lines are open from 9am to 5pm, Monday to Friday.
What happens if you are not PCI DSS compliant	If you are not compliant with PCI DSS, we will charge you a non-compliance charge per month, per outlet, until you confirm your compliance. This is currently £20. This charge will be applied to your account if you are not compliant within three months from the date you receive your PCI DSS portal login details.

Please contact us if you'd like this in an alternative format such as Braille, large print or audio.

Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service.