>> View all legal agreements

PayPal Website Payments Pro and Virtual Terminal Agreement

Last Update: Dec 11, 2018

Print Download PDF

This PayPal Website Payments Pro / Virtual Terminal Agreement ("Agreement") is a contract between you (also referred to as the “Merchant”) and PayPal (Europe) S.àr.l. et Cie, S.C.A. ("PayPal" or "we"). You agree that any use by you of Online Card Payment Services shall constitute your acceptance of this Agreement and we recommend that you store or print-off a copy of this Agreement. PayPal is licensed as a Luxembourg credit institution and is under the prudential supervision of the Luxembourg supervisory authority, the Commission de Surveillance du Secteur Financier (the "CSSF"). The CSSF has its registered office in L-1150 Luxembourg. Because the funds in your PayPal Account are electronic money, which does not legally qualify as a deposit or an investment service, you are not protected by the Luxembourg deposit guarantee schemes provided by the Association pour la Garantie des Dépôts Luxembourg.

This Agreement applies to your use of PayPal Website Payments Pro and/or Virtual Terminal (the "Products"). To proceed with obtaining one or both of the Products, you must read, agree with and accept all of the terms and conditions contained in this Agreement.

We may make Changes to this Agreement by giving notice of such Change by posting a revised version of this Agreement on the PayPal website(s). A Change will be made unilaterally by us and you will be deemed to have accepted the Change after you have received notice of it. We will give you 2 months' notice of any Change with the Change taking effect once the 2 month notice period has passed, except the 2 month notice period will not apply where a Change relates to the addition of a new service, extra functionality to the existing Service or any

other change which neither reduces your rights nor increases your responsibilities. In such instances, the change will be made without notice to you and shall be effective immediately upon giving notice of it. All future Changes set out in the **Policy Update** already published on the "Legal Agreements" landing page of the PayPal website at the time you register for the Online Card Payment Services are incorporated by reference into this Agreement and will take effect as specified in that **Policy Update**.

If you do not accept any Change, you must close your Account following the account closure procedure set out in **this Agreement**. If you do not object to a Change by closing your Account within the 2 month notice period, you will be deemed to have accepted the Change. While you may close your Account without charge, please note that you may still be liable to us after you terminate this Agreement for any liabilities you may have incurred and are responsible for prior to terminating this Agreement and please further note our rights under the User Agreement.

Capitalised terms are defined below. Please view **download and save** this agreement.

1. Setting up and activating your Product

1. **Getting started.** To obtain and use your Product, you must first do all of the following:
    a. Complete the online application and approval process for your Product, open a PayPal Business Account (if you do not already have one), and follow the instructions set out in PayPal's online process to access and use your Product.
    b. Integrate your Product into the payment process of your website, if your Product is Website Payments Pro. You are not required to integrate your Product into the payment process of your website if you only access and use Virtual Terminal. PayPal is not responsible for any problems that could occur by integrating your Product into your 'live' website.
    c. Activate your Product by using it in a 'live' payment transaction for the first time.

If your Product is Website Payments Pro, you may only integrate and use Website Payments Pro in one of the following mutually exclusive ways -

either (i) as a PayPal Hosted Solution (in which PayPal operates Website Payments Pro for you as a PayPal-hosted service) or (ii) operated on your own facilities - (each option being a **"Hosting Option")**. PayPal may (but, notwithstanding any other provision in this Agreement, shall not be obliged to) provide both Hosting Options. PayPal may, at its sole discretion, set either Hosting Option as your default option for integrating the Direct Payments API into the payment process of your website.

2. **Required use of Express Checkout.** If your Product is Website Payments Pro, you must implement PayPal Express Checkout as part of your website integration; see clause 2(1) below. In implementing Express Checkout, you agree that your website:
    a. Includes a PayPal Express Checkout button either: (A) before you request the shipping/billing address and other financial information from your customers or (B) on the same page that you collect such information if you only use one page for your checkout process.
    b. Offers PayPal as a payment option together with the other payment options you offer for Express Checkout. The PayPal logo must be displayed with equal or greater prominence as the logos for your other payment options.
    c. Provides your customers with the option of not storing their personal information, including their email address, shipping/billing address, and financial information, as part of the checkout process.

    Failure to implement Express Checkout affects the fees you pay; see clause 2(1) and 2(3).

3. **Your information.** You confirm that you have read, consented and agreed to PayPal's Privacy Policy, which explains the information that we collect about you and your online business. In particular, you agree and consent that PayPal may obtain from a third party your credit history and financial information about your ability to perform your obligations under this Agreement; the PayPal Privacy Policy lists the companies involved in this exchange of credit-related information. PayPal will review your credit and other risk factors of your Account (reversals and chargebacks, customer complaints, claims etc.) on an ongoing basis, and we may also review your website and the products for sale on it. PayPal will store, use and disclose all information that we have about you in conformity with PayPal's Privacy Policy.

5. **Cancellation.** PayPal may terminate your access to and/or use of either or both Products and / or terminate this Agreement at any time before the Activation Date by notifying you.

2. Fees

1. **How fees are paid**. You agree to pay the fees in this Agreement as they become due without set-off or deduction. You authorise PayPal to (and PayPal may) collect Monthly Fees first from any available Balance in your Account and then also from the funding source(s) registered for your Account, and you authorise PayPal to (and PayPal may) collect fees for receiving payments from the payments you receive before those funds are credited to your account. If PayPal is unable to collect a past due fee from your Account and its funding source(s), we may take action against you as provided in the User Agreement for unpaid fees.

   Except as further provided in this Agreement, you agree to pay the fees set out in the User Agreement.

   Fees will be charged in the currency of the payment received.

   See the Glossary at clause 2.6 for further reference.

2. **Monthly Fees**

Product	**Monthly Fee**
Website Payments Pro (including Express Checkout, Direct Payments API, Virtual Terminal and Fraud Management Filters)	GBP 20.00
Virtual Terminal only	GBP 20.00

3.

3. **Transaction Fees for Standard PayPal Payments with Express Checkout**

		the PayPal Merchant Rate is as follows:

If you receive the payment:	the PayPal Standard Rate fee is:	where the aggregate monetary amount of payments received in your PayPal Account in the previous calendar month is:	the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:
as a Standard PayPal Payment using Express Checkout	3.4% + Fixed Fee	GBP 0.00 - GBP 1,500.00	3.4% + Fixed Fee
		GBP 1,500.01 - GBP 6,000.00	2.9% + Fixed Fee
		GBP 6,000.01 - GBP 15,000.00	2.4% + Fixed Fee
		GBP 15,000.01 – GBP 55,000.00	1.9 % + Fixed Fee
		Above GBP 55,000.00	1.4 % + Fixed Fee

4.

4. **Transaction Fees for Card Payments under the Blended Pricing Fee Structure**

If you receive a payment:	the PayPal Standard Rate fee is:	the PayPal Merchant Rate is as follows:	
		where the aggregate monetary amount of payments received in your PayPal Account in the previous calendar month is:	the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:
from a card (Visa, MasterCard or		GBP 0.00 - GBP 1,500.00	3.4% + Fixed Fee

Maestro) using the Online Card Payment Services	3.4% + Fixed Fee	GBP 1,500.01 - GBP 6,000.00	2.9% + Fixed Fee
		GBP 6,000.01 - GBP 15,000.00	2.4% + Fixed Fee
		Above GBP 15,000.00	1.9 % + Fixed Fee

5.

5. **Transaction Fees for Card Payments under the Interchange Plus Fee Structure**

If you receive a payment:	**the PayPal Standard Rate fee is:**	**the PayPal Merchant Rate is as follows:**	
		where the aggregate monetary amount of payments received in your Account in the previous calendar month is:	**the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:**
from a card (Visa, MasterCard or Maestro) using the Online Card Payment Services	Interchange Fee (approximately ranges from 0.2% to 2.0%) + 2.9% + Fixed Fee	GBP 0.00 - GBP 1,500.00	Interchange Fee + 2.9% + Fixed Fee
		GBP 1,500.01 - GBP 6,000.00	Interchange Fee + 2.4% + Fixed Fee
		GBP 6,000.01 - GBP 15,000.00	Interchange Fee + 1.9% + Fixed Fee
		Above GBP 15,000.00	Interchange Fee + 1.4% + Fixed Fee

6.

6. **Glossary**

a. Interchange Fees are set by Visa and MasterCard. They approximately range from 0.2% to 2.0% and vary for different types of cards (for example by categories and brand). **PayPal shall always charge you the Interchange Fee as set by Visa and MasterCard and as passed on by its Acquirer.** Single Interchange Fees may change from time to time. For more information on Interchange Fees, please see **MasterCard's** and **Visa's**website as well as our **simplified overview**.

b. Percentage-based fees (such as 3.4%) refer to an amount equal to that percentage of the payment amount.

c. Fixed Fees are based on the currency received, as follows:

Argentine Peso:	2.00 ARS	New Zealand Dollar:	$0.45 NZD
Australian Dollar:	$0.30 AUD	Norwegian Krone:	2.80 NOK
Brazilian Real:	0.60 BRL	Philippine Peso:	15.00 PHP
Canadian Dollar:	$0.30 CAD	Polish Zloty:	1.35 PLN
Czech Koruna:	10.00 CZK	Russian Ruble	10.00 RUB
Euro:	€0.35 EUR	Singapore Dollar:	0.50 SGD
Danish Kroner:	2.60 DKK	Swedish Kronor:	3.25 SEK
Hong Kong Dollar:	$2.35 HKD	Swiss Franc:	0.55 CHF
Hungarian Forint:	90 HUF	Taiwan New Dollar:	10.00 TWD
Israeli New Shekels:	1.20 ILS	Thai Baht:	11.00 THB
Japanese Yen:	¥40 JPY	Turkish Lira:	0.45 TRY
Malaysian Ringgit:	2 MYR	**UK Pounds Sterling:**	**£0.20 GBP**
Mexican Peso:	4.00 MXN	US Dollar:	$0.30 USD

7.

7. **Blended Pricing or Interchange Plus Transaction Fees?**

When you receive card payments using any of our Online Card Payment Services (including via Direct Payment API or Virtual Terminal):

a. The Blended Pricing fee structure shall apply until 23 June 2016 ("**Interchange Plus Launch**").
b. You may choose the fee structure applicable to you on or after Interchange Plus Launch, by the methods or procedures that PayPal may make available to you before and after Interchange Plus Launch. If you do not make an election, you will stay on your existing fee structure.
c. You may choose your fee structure for future transactions only, not for past transactions. The fee structure that applies when you receive card payments using any of our Online Card Payment Services also applies when you receive card payments using PayPal Here™. This means that if you opt to be charged under the Interchange Plus fee structure, the respective Interchange Plus fee structure will apply to the use of both our Online Card Payment Services and PayPal Here.

8. **Merchant Rate**

Merchant Rate applies only to Accounts with Merchant Rate status. Merchant Rate status is subject to eligibility, application and approval by PayPal. PayPal may evaluate applications on a case-by-case basis, including, without limitation, on the following criteria: qualifying monthly sales volume, size of average shopping cart and an Account in good standing. To be eligible to apply for (and retain) PayPal Merchant Rate status the Account must:

- at all times be in good standing and not under investigation; and
- have received more than £1,500.00 GBP in aggregate monetary amount of payments in the previous calendar month.

PayPal may downgrade an Account to the Standard Rate at any time if the above conditions are not met or there are unresolved chargebacks against the Account or as otherwise provided for under the provisions relating to the Merchant Rate in the User Agreement.

If PayPal downgrades your Account you will need to apply to PayPal again for your Account to get Merchant Rate status.

You may apply to receive Merchant Rate for your Account using the dedicated online **application form** when logged into your PayPal Account. If your application is rejected, please note that you may only submit an application once every thirty days.

9. **Additional Transaction Fees**

a. Receiving Cross Border Payments

The fee for Receiving Cross Border payments applies as outlined in the User Agreement, except that it does not apply to payments received from **cards using the Online Card Payment Services under the Interchange Plus fee structure**.

b. Failure to implement Express Checkout. If you do not implement Express Checkout as required in clause 1 (2) above, the percentage components of the Transaction Fees set out in clause 2.2 will each increase by an additional 0.5 % after PayPal gives you 30 days' notice. You agree to pay the increased fees.

c. Additional risk factors. If PayPal determines that your Account receives, or is likely to receive, a disproportionately high number of customer complaints, Reversals, Chargebacks, Claims, or other indicators of a serious level of risk, PayPal may increase the percentage components of your Transaction Fees by up to 5%, after giving you 30 days prior notice of the increase. You agree to terminate your use of the Product if you do not agree to this increase.

10. **Other Fees**

Activity/Event/Product	Fee
. **Recurring Payment Tool (optional service)**	GBP 20.00 per month
b. **Uncaptured Authorisation Transactions**	GBP 0.20 for each successful but uncaptured authorisation transaction via Direct Payment API or Virtual Terminal
c. **Card Account Verification Transactions**	0.20 GBP

	for each card account verification request (for all Direct Payment API or Virtual Terminal card account verification transactions (Visa and MasterCard only). For the avoidance of doubt, this does not include Uncaptured Authorisation Transactions.

11. **MasterCard transactions**. For further information about MasterCard's rules and rates, please visit: **http://www.mastercard.com/us/merchant/index.html**.

12. **Monthly Reports on Transaction Costs**. PayPal shall make available monthly reports on transaction costs (inclusive of interchange fees) for card transactions which you process with PayPal Website Payments Pro and Virtual Terminal. These reports will be downloadable from your PayPal Account. The reports do not include any Standard PayPal payments.

3. Settlement of Card Payments within the Interchange Plus Fee Structure

You agree that, when PayPal receives a card payment for you, PayPal may hold those funds in your Reserve Account and you are thereby giving a Payment Order that instructs PayPal to pay those funds to your Payment Account only on the Business Day on which PayPal receives the information about the interchange fee applicable to the card payment, at which time the funds will then be made available to you in your Payment Account. While the funds are held in your Reserve Account, the transaction will appear to you as "Pending" in your Account details. PayPal does not consider that the proceeds of the card payment in your Reserve Account are at your disposal until PayPal has received the information on the applicable interchange fee from our Processor (which can be within the next Business Day following the day on which the card payment was initiated by the card holder).

4. Information security; Data Protection

1. **Compliance with Data Security Schedule**. You agree (as a "Merchant") to comply with Schedule 1 below, which forms part of this Agreement.

2. **Your PCI DSS compliance**. You also agree to comply with the PCI Data Security Standard (PCI DSS). You must protect all Card Data that comes within your control according to PCI DSS, and you must design, maintain and operate your website and other systems in conformity with PCI DSS. You must ensure that your staff are and remain sufficiently trained so that they are aware of PCI DSS and can carry out its requirements. PayPal is not responsible for any costs that you incur in complying with PCI DSS.
3. **PayPal's PCI DSS compliance**. PayPal warrants that PayPal and your Product comply and will comply with PCI DSS. However, PayPal's compliance, and your Product's, are not sufficient to achieve compliance with PCI DSS by you and your systems and processes.
4. **3D Secure**. Requirements of the European Central Bank and PayPal's bank regulators require use of 3D Secure in certain circumstances, and Card Associations may also require it to reduce an excessive number of Card Transactions unauthorised by the cardholder. PayPal may by notice to you require that you implement 3D Secure for all or certain specified Card Transactions. You agree to implement 3D Secure if required in such a notice, where the issuer of a particular card supports 3D Secure for that card.
5. **Price and currency**. You may not submit payment transactions in which the amount is the result of dynamic currency conversion. This means that you may not list an item in one currency and then accept payment in a different currency. If you are accepting payments in more than one currency, you must separately list the price for each currency.
6. **Compliance with Data Protection Schedule.** You agree (as a "Merchant") to comply with Schedule 2 below, which forms part of this Agreement. The terms of the Data Protection Schedule prevail over any conflicting terms in this Agreement relating to data protection and privacy.

5. User Agreement

1. **User Agreement applies**. You acknowledge and agree that the User Agreement, and not this Agreement, is the "framework contract" between you and PayPal as defined in laws transposing the Second Payment Services Directive ((EU)2015/2366). The terms of the User Agreement also apply to you and are incorporated by reference into this Agreement. The definition of "Services" in the User Agreement shall be amended to include your Product, and the definition of "Agreement" shall include this Agreement. In case of any inconsistency between this Agreement and the User Agreement, this Agreement supersedes the User Agreement, but only to the extent of that inconsistency. Where this Agreement and the

User Agreement both specify a fee for the same action, the fee specified in this Agreement will apply rather than the fee in the User Agreement. The User Agreement can be found via a link in the footer of nearly every PayPal web page. The User Agreement includes important provisions which:

a. Permit PayPal to take a Reserve to secure your obligation to pay Chargebacks, Reversals and fees;
b. Obligate you to follow PayPal's Acceptable Use Policy in your use of PayPal;
c. Give legal effect to PayPal's Privacy Policy, which governs our use and disclosure of your information and that of Shared Customers; and
d. Permit PayPal to restrict a payment or your PayPal Account in circumstances listed in the User Agreement.

2. **Failed payments and Product tools**. You are responsible for Chargebacks, Reversals and other invalidated payments as provided in the User Agreement, regardless of how you use and configure your Product, including its fraud filtering technology and similar preventive tools (if any). Those tools can be useful in detecting fraud and avoiding payment failures, but they do not affect your responsibility and liability pursuant to the User Agreement for Chargebacks, Reversals and payments which are otherwise invalidated.

6. Intellectual property and ID codes

1. **Licence**. PayPal hereby grants to you a non-exclusive, non-transferable, revocable, non-sublicenseable, limited license to (a) use your Product in accordance with the documentation provided on the PayPal Website; and to (b) use the documentation provided by PayPal for your Product and reproduce it for internal use only within your business. Your Product as licensed is subject to change and will evolve along with the rest of the PayPal system; see clause 8(1). You must comply with the implementation and use requirements contained in all PayPal documentation and instructions accompanying the Product issued by PayPal from time to time (including, without limitation, any implementation and use requirements we impose on you to comply with applicable laws and card scheme rules and regulations).
2. **ID codes**. PayPal will provide you with certain identifying codes specific to you. The codes identify you and authenticate your messages and instructions to us, including operational instructions to PayPal software interfaces. Use of the codes may be necessary for the PayPal system to process instructions from you (or your website). You must keep the codes

safe and protect them from disclosure to parties whom you have not authorised to act on your behalf in dealing with PayPal. You agree to follow reasonable safeguards advised by PayPal from time to time in order to protect the security of those identifying codes. If you fail to protect the security of the codes as advised, you must notify PayPal as soon as possible, so that PayPal can cancel and re-issue the codes. PayPal may also cancel and re-issue the codes if it has reason to believe that their security has been compromised, and after notifying you whenever notice can reasonably be given.

3. **Ownership of PayPal Website Payments Pro information and materials**. As part of Merchant's access to, and utilisation of PayPal Website Payments Pro, Merchant will be provided with certain information and materials (the "Pro Materials") which are able to be used by Merchant to use PayPal Website Payments Pro. All intellectual property rights associated with the Pro Materials remain the property of PayPal or the relevant Acquiring Institution(as the case may be). Merchant agrees to not give, transfer, assign, novate, sell, resell (either partly or in whole) the Pro Materials to any person.

7. Banking terms for Card Transactions

1. PayPal utilises services from banking partners in processing Card Transactions, including both direct payments to you from a card as well as Card Transactions that fund a PayPal payment to you. The **Commercial Entity Agreements** apply in relation to those services. In accepting this Agreement, you also accept the **Commercial Entity Agreements**, which form part of this Agreement. A copy of the Commercial Entity Agreements can be obtained from the Legal link at the bottom of a PayPal web page.

8. Termination and suspension

1. **By you**. You may terminate this Agreement by giving 30 days' prior notice to PayPal Customer Service of your intent to either:
    a. terminate this Agreement. PayPal Customer Service will confirm termination via email. This option lets you stop using your Product and paying for it, but your PayPal Account remains open and its User Agreement remains in effect; or
    b. close the PayPal Account that you use with your Product (see the User Agreement for more information). This option terminates this Agreement, letting you stop using your Product and paying for it, and initiates the closure process for your PayPal Account. Your PayPal

Account remains open and its User Agreement remains in effect until the closure of the PayPal Account takes effect, subject further to the provisions relating to closing your PayPal Account in the User Agreement.

2. **By PayPal**. PayPal may terminate this Agreement by doing any of the following:
    a. Giving you 2 months' notice by email to you at your registered email address associated with your Account of PayPal's intent to terminate this Agreement. Unless otherwise notified, terminating this Agreement does not affect your User Agreement and your PayPal Account remains open.
    b. Terminating the User Agreement that applies to the PayPal Account used with your Product.
3. **By events**. PayPal may terminate this Agreement immediately without notice if you:
    a. Breach this Agreement or the User Agreement;
    b. Become unable to pay or perform your obligations as they fall due;
    c. Become unable to pay your debts (within the meaning of section 123 of the Insolvency Act 1986), admit your inability to pay your debts or otherwise become insolvent;
    d. Have any distraint, execution, attachment or similar action taken, levied or enforced against you or your assets, or if any garnishee order is issued or served on you;
    e. Become the subject of any petition presented, order made or resolution passed for the liquidation, administration, bankruptcy or dissolution of all or a substantial part of your business, except where solvent amalgamation or reorganisation is proposed on terms previously approved by PayPal,
    f. Lose full and unrestricted control over all or part of your assets because of the appointment of a receiver, manager, trustee, liquidator or similar officer;
    g. Enter into or proposes any composition or arrangement concerning your debts with your creditors (or any class of its creditors);
    h. A material adverse change occurs in your business, operations, or financial condition; or
    i. You provide inaccurate information in applying for your Product or in your dealings with us.
4. **Effect of termination**. When this Agreement terminates, you must immediately stop using your Product, and PayPal may prevent or hinder you from using it after termination. If you nevertheless use a Product after termination of this Agreement, then this Agreement will continue to apply to your use of that Product until you give effect to the termination by stopping your use of that Product. The following clauses in this Agreement shall

survive termination of this agreement and continue in full force and effect: Clauses 2, 4(1) 8(2), 8(4). Termination of this agreement shall not affect any rights, remedies or obligations of the parties that have accrued or become due prior to termination, and you will not be entitled to a refund of any Monthly Fee applicable to any period prior to termination.

5. **Breach and suspension**. If you breach this Agreement, the User Agreement, or a security requirement imposed by PCI DSS, PayPal may immediately suspend your use of your Product (in other words, we may render your Product temporarily inoperable). PayPal may require you to take specified corrective actions to cure the breach and have the suspension lifted, although nothing in this Agreement precludes PayPal from pursuing any other remedies it may have for breach. In addition, if PayPal reasonably suspects that you may be in breach of this Agreement or PCI DSS, PayPal may suspend your use of your Product pending further investigation.

   If PayPal suspends your access to or use of PayPal Website Payments Pro, PayPal will notify you and explain the basis of PayPal's actions in suspending your use of your Product, and may specify corrective actions to cure the breach and have the suspension lifted. PayPal's suspension of the Merchant's access or use of PayPal Website Payments Pro will remain in effect and until such time as PayPal is satisfied that the Merchant has remedied the applicable breach(es).

9. Miscellaneous

1. **Future of the Products**. PayPal retains sole and absolute discretion in determining (a) the future course and development of the Products, (b) which improvements to make in them and when, and (c) whether and when defects are to be corrected and new features introduced. PayPal welcomes feedback from users in planning the future of the Products but is not required to act in accordance with any feedback received. In giving us feedback, you agree to claim no intellectual property interest in your feedback.
2. **No warranty**. Your Product and all accompanying documentation are provided to you on an "as is" basis. PayPal does not give or offer any warranty, express or implied, by operation of law or otherwise, in relation to your Product, the licensed software or user documentation provided. Nothing provided by PayPal under this Agreement or otherwise for your Product has PayPal's authorisation to include a warranty, and no obligation or liability will arise out of PayPal's rendering of technical, programming or other advice or service in connection with any Product, licensed software

and user document provided (including, without limitation, services that may assist you with the customisation of your Product). PayPal recommends that you test the implementation of your Product thoroughly as PayPal is not responsible for any loss caused by a defect in it.

If PayPal hosts your Product (in other words, we run the software for you as a web service), PayPal does not guarantee continuous, uninterrupted or secure access to your hosted Product. PayPal will not be liable for any delay or failure in hosting your Product. You acknowledge the availability of your Product for use may be occasionally limited to allow for repairs, maintenance or the introduction of new facilities or services.

3. **Indemnity**. You agree to indemnify PayPal and keep PayPal fully indemnified on a continuing basis from any direct loss, damage and liability, and from any claim, demand or cost (including reasonable attorneys' fees) incurred in relation to any third party (including a Shared Customer) and arising out of your breach of this Agreement, the User Agreement and the documents incorporated in it by reference (including the Acceptable Use Policy), or the violation of any law.

4. **PayPal Hosted Solution and your intellectual property**. You hereby grant to PayPal a royalty-free, worldwide non-exclusive licence to use your or any of your affiliates' names, images, logos, trademarks, service marks, and/or trade names as you may provide to PayPal when using the Products ("Your Marks") for the sole purpose of enabling your use of the Products (including, without limitation, the customisation of your hosted Product). Title to and ownership of Your Marks and all goodwill arising from any use hereunder will remain with you. You represent and warrant that you have the authority to grant PayPal the right to use Your Marks and you shall indemnify PayPal and keep PayPal fully indemnified on a continuing basis from any claims or losses suffered by it arising from the use of Your Marks in connection with the Products.

5. **Assignment, amendment and waiver**. You may not assign this Agreement without first obtaining PayPal's written consent. PayPal may assign, novate or otherwise transfer this agreement without your consent by notifying you. Neither party may amend this Agreement or waive any rights under it except in a written document signed by both parties.

6. **English law and jurisdiction**. This Agreement is governed by English law. The parties submit to the non-exclusive jurisdiction of the courts of England and Wales.

10. Definitions

Capitalised terms not listed in this clause are defined in the User Agreement.

1. **3D Secure**: A security procedure that enables a card-issuing bank to authenticate the cardholder authorising a Card Transaction at the time a payment is made. 3D Secure has other brand names depending on the Card Association whose branding appears on the card; brand names for 3D Secure include Verified by Visa and MasterCard SecureCode.
2. **Account Nationality**: The "Account Nationality" of a PayPal Account is the same as that of the bank account into which PayPal E-money is withdrawn (redeemed). For example, if a Spanish bank account is registered as the account into which PayPal E-money is withdrawn, then the Account Nationality of the PayPal Account from which that redemption occurs is Spanish. A PayPal Account from which E-money is withdrawn into a German bank account would be German, even though a German and Spanish Account would both be denominated in the same currency (Euros).
3. **Acquiring Institution:** means a financial institution or bank that provides services to you and PayPal to enable you to (a) accept payment by cardholders using cards: and (b) receive value in respect of Card Transactions.
4. **Activation Date**: The date on which you complete all of the steps for “Getting started” as listed in clause 1(1) above.
5. **Advanced Fraud Management Filters** : Technology provided by PayPal to enable you to (a) check a card payment against criteria such as the cardholder’s billing address (Address Verification Service or AVS), the card’s CVV2 Data, and databases of suspicious addresses, identifiers, and patterns. See the PayPal Website and product documentation for further information. Advanced Fraud Management Filters offer a greater level of transaction screening, and transactions can be automatically flagged, reviewed or declined based on how you configure the filters.
6. **AVS Data**: Information returned by the Address Verification System operated by or on behalf of Card Associations, which compares address data provided by an apparent cardholder with address data on file for the card at the card issuer.
7. **Card Association**: A company or consortium of financial institutions which promulgates rules to govern Card Transactions that involve the card that carries the company’s or the consortium’s brand. Examples include Visa USA, Visa Europe, and the other Visa regions; Mastercard International Incorporated; American Express Company and similar organisations.

8. **Card Data**: All personal or financial information relevant to a Card Transaction, including information recorded on the card itself (whether in human-readable form or digitally), together with the cardholder's name and address and any other information necessary for processing a Card Transaction.
9. **Card Transaction**: A payment made using a credit or debit card, an American Express card, or any other payment method using a physical data-carrying item intended to be held in the payer's possession. The Products support only certain types of Card Transactions; see the PayPal Website for more information.
10. **Critical Systems**: The information technology (both hardware and software) that you employ to operate your Products, to protect them and your online points of sale against intrusion and interference, and to store payment-related and personal data, including any Card Data that you retain and all personal data about Shared Customers.
11. **CVV2 Data**: The three-digit number printed to the right of the card number in the signature panel area on the back of the card. (For American Express cards, the code is a four-digit unembossed number printed above the card number on the front of the American Express card.) The CVV2 Data are uniquely associated with each individual plastic card and ties the card account number to the plastic.
12. **Data Breach**: An intrusion into or malfunction of a computer system in which Card Data are stored, and which intrusion or malfunction either (a) exposes, modifies or destroys all or part of the Card Data in the system, or (b) runs a significant risk, in the opinion of a qualified expert in information security, of exposing, modifying or destroying all or part of the Card Data in the system. Card Data are exposed where they are released from the normal access controls of the system without authorisation, or where they are actually disclosed to one or more unauthorised persons.
13. **Data Protection Directive**: European Union Directive 95/46/EC or any successor to it, together with all other laws about the privacy of citizens or residents of the member state of the European Economic Area in which you reside or are established as a business enterprise.
14. **Direct Payments API**: Functionality for performing credit and debit card transactions, where the card details are entered online by the cardholder.
15. **Express Checkout**: Functionality for expediting online retail checkout by using information provided to you by PayPal. Details about Express Checkout appear on the **PayPal Website** and in the documentation that PayPal provides for Website Payments Pro.
16. **Hosting Option**: As defined in 1(1) above.
17. **Monthly Fee**: A fee payable on a monthly basis as required in clause 2 above.

18. **Online Card Payment Services**: Functionality provided online by PayPal to enable merchants to receive payments directly from a payer's card (without the funds passing via the payer's PayPal Account), without the card being present at the website or other point of sale. Online Card Payment Services are integral to the Products such as Direct Payments API and Virtual Terminal. PayPal Here™ is not an Online Card Payment Service because the card is present at a physical point of sale.
19. **PayPal Hosted Solution**: PayPal's Direct Payments API integrated into the payment process of your website pursuant to clause 1(1), with that API being operated entirely on PayPal's server (rather than on your website).
20. **PayPal Website**: The website provided by PayPal for the country in which you reside. In the case of the UK, the PayPal Website is currently at http://www.paypal.co.uk. References to PayPal Websites for other countries can be found via a link from any other PayPal Website.
21. **PCI DSS**: Payment Card Industry Data Security Standard, which consists of specifications prescribed by Card Associations to ensure the data security of Card Transactions. A copy of PCI DSS is available online from **https://www.pcisecuritystandards.org/**.
22. **Product**: "Your Product" means whichever one of the Products you access and use after accepting this Agreement.
23. **Qualified Security Assessor** has the meaning given it in PCI DSS.
24. **Recurring Payments Tool**: Technology provided by PayPal for setting up payments that recur at specified intervals or frequencies with authorisation from the payer. See the PayPal Website and product documentation for further information.
25. **Shared Customer**: A person who both has a PayPal Account and is also your customer.
26. **Standard PayPal Payments**: All Payments which you receive from another PayPal account or payments via PayPal's Account Optional Service.
27. **User Agreement**: The contract entered into online as part of the online registration process required to open a PayPal Account. The current User Agreement is to be found via a link from the footer of nearly every page on the PayPal Website. It includes certain policies, notably the Acceptable Use Policy and Privacy Policy, which are also listed on the PayPal Website.
28. **Virtual Terminal**: Functionality provided by PayPal to enable you to receive a card payment by manually entering Card Data given you by the cardholder. Virtual Terminal is one of the Online Card Payment Services
29. **Website Payments Pro**: A suite of functionality consisting of Express Checkout, Direct Payments API, Virtual Terminal and Fraud Management Filters as standard. Optional additional services include

Advanced Fraud Management Filters and the Recurring Payments Tool. Website Payments Pro is one of the Online Card Payment Services.

Schedule 1
Data Security Requirements

Website Payment Pro and Virtual Terminal enable you to accept payments online directly from debit and credit cards, which are payment instruments whose security depends on controlling the disclosure of Card Data. A person who has sufficient Card Data can send or receive a card payment charged to the cardholder's account without necessarily having the cardholder's authorisation for the payment. To prevent your Shared Customers from having their Card Data misused, you must keep Card Data secret at all times. Laws transposing the Data Protection Directive also require you to keep a Shared Customer's personal data secure.

PayPal strongly recommends that you obtain the services of a competent professional expert in information security to advise you and assist in securing your website and any other points of sale.

Principles of Data Security

1. **Design and development**. You must design and develop your Critical Systems and all payment-related processes so that they are secure from intrusion and interference by unauthorised persons. All users of your systems must be required to authenticate themselves to your Critical Systems, and those Systems must limit the access and powers of their users. You must also organise your business so as to segregate critical duties and create controls and checkpoints in your operations, rather than place too much unchecked power over your systems and operations in one person. Never give a user more power over your systems and processes than the minimum necessary for the user to perform his or her assigned role.
2. **Protection against intrusion**. You must divide your operations into two basic categories, (1) those functions available to all users including those outside your organisation, and (2) those available only to trusted people within your organisation. You must employ a firewall to block untrusted users from the using internal-only functions of your Critical Systems. Your

web servers and other external-facing portions of your Critical Systems must use well developed and thoroughly tested technology, and make available externally only those functions which are necessary for Shared Customers and other external users to use. Strip your external-facing servers of all superfluous functions to protect (harden) them and reduce their vulnerability to external attack.

3. **Access controls**. Your Critical Systems must restrict access to Card Data and all other personal or important data to only trusted persons within your organisation, and no such person should have greater access to such data than is necessary for that person to perform his or her role. Your systems must track and log all access, use, modification and deletion of Card Data and other personal or important data so that you maintain an audit trail of all such actions. You must also limit access to your Critical Systems and the resources on which they depend such as networks, firewalls, and databases.
4. **Data minimisation**. As a general principle, you should gather and retain no more Card Data or other sensitive data than you need. Holding Card Data and personal data creates a risk of liability to you, and you can reduce that risk by taking and holding less data. If you store Card Data, consider carefully the need to do so: PayPal must refund a payment which lacks its payer's authorisation, and if the user will authorise a further payment, the user will generally also give you up-to-date Card Data again, so you may have little need to store Card Data for future use. Card Data that you do not have is data that you cannot spill if you suffer a Data Breach.
5. **Changes and testing**. Except in emergencies, avoid changing Critical Systems without first planning, testing, and documenting the change, unless the change is routine (*e.g.* adding a user, changing a password, updating inventory and prices). For major systemic changes or those which can impact the security or availability of your Critical Systems, planned changes should be escalated for approval by high-ranking managers other than the planners of those changes. Implement planned changes in your production systems only after they have been thoroughly tested in a non production environment. Conduct all such testing under the supervision of the your risk management department or others in your company with particular responsibility for its losses.
6. **Audits**. You must audit the operations and security of your Critical Systems at least once a year. This systems audit must be distinct from any audit of your finances. Use trusted and independent experts to audit your Critical Systems, and if you use your employees as auditors, ensure their independence by protecting their employment from retaliation and by isolating them from the work of administering, operating, changing and testing your Critical Systems.

7. **Outsourcing and organisational control**. You must ensure that all persons who have access to your Critical Systems, or who design, develop, operate, maintain, change, test and audit your Critical Systems comply with this Agreement and PCI DSS. You are responsible to ensure compliance even if such persons are not your employees.

What to do in case of a Data Breach

8. **Data Breach**. If you experience a Data Breach, you agree to do all of the following:
    a. Take whatever action you can to stop the Data Breach and mitigate its consequences immediately after discovering the Data Breach.
    b. Notify PayPal as soon as possible after discovering the Data Breach by contacting your account manager (if one is assigned to you) or contacting our Customer Service (details of how to contact us are on the **"Contact Us"** page). If you cannot simultaneously do (a) and notify PayPal, then do (a) first and then notify PayPal.
    c. Notify all Shared Customers whose Card Data has been exposed or which is likely to have been exposed, so that those Shared Customers can take steps to prevent misuse of the Card Data. You further agree to complete this notification immediately after you perform (a) and (b) above, to notify PayPal when you have completed this notification, and to provide a list of Shared Customers whom you have notified. If you fail to complete this step promptly after the Data Breach, PayPal may notify Shared Customers of the Data Breach, and will identify the Shared Customers from your PayPal Account records of who has paid you using a card.
    d. If requested by PayPal, have an independent third party auditor, approved by PayPal, conduct a security audit of your Critical Systems and issue a report. You agree to comply with PayPal's request under this clause at your own expense. You must provide a copy of the auditor's report to PayPal, and PayPal may provide copies of it to the banks (including, without limitation, Acquiring Institutions) and Card Associations involved in processing card transactions for PayPal. If you do not initiate a security audit with 10 business days of PayPal's request, PayPal may conduct or obtain such an audit at your expense. See also Schedule 1 on Audit.
    e. Cooperate with PayPal and follow all reasonable instructions from PayPal to avoid or mitigate consequences of the Data Breach, to improve your Critical Systems so that they satisfy the requirements this Agreement, and to help prevent future Data Breaches. However, PayPal shall not require you to do more than this Agreement requires, unless the additional measures are

reasonable in light of the risk to Shared Customers and the best practices of online retailing.

f. Resume normal operation of your Critical Systems only when you have ascertained how the Data Breach occurred and taken all reasonable steps to eliminate the vulnerabilities that made the Data Breach possible or which could make other Data Breaches possible;
g. Report the Data Breach to law enforcement authorities, cooperate in any investigation that they undertake, and cooperate as the authorities may request in order to identify and apprehend the perpetrator of the Data Breach.
h. Refrain from using Card Data that have been exposed or modified in the Data Breach. However, this clause does not prevent you from obtaining and using Card Data again from Shared Customers affected by the Data Breach, after the vulnerabilities in your Critical Systems have been remedied pursuant to (f) above.

Data protection

9. **See Schedule 2 for Data Protection terms.**

10. **Intentionally left blank.**

Card Data and PCI DSS

11. **Retention of Card Data**. Unless you receive and record the express consent of the cardholder, you may not retain, track, monitor or store any Card Data. You must completely and securely destroy all Card Data that you retain or hold within 24 hours after you receive an authorisation decision from the issuer relevant to that Card Data.

If, with the cardholder's consent, you briefly retain Card Data, you may do so only to the extent that the Card Data are necessary for processing payment transactions with the cardholder's authorisation. You must never give or disclose the retained Card Data to anyone, not even as part of the sale of your business. Moreover, and regardless of anything to the contrary, you must never retain or disclose the card verification and identification data printed in the signature stripe on the back of the card (i.e. the CVV2 Data), not even with the cardholder's consent.

12. **Card Data that you must not store**. Notwithstanding the immediately preceding clause, you agree to not store any personal

identification number (PIN) data, AVS Data, CVV2 Data, or data obtained from the magnetic stripe or other digital storage facility on the card (unless that data is also printed or embossed on the front of the card) of any cardholder. Card associations may impose fines if you violate this clause, which reflects card association rules. In this clause, 'store' means retain in any form, whether digital, electronic, paper-based, or otherwise, but does not include temporary capture and holding of data while it is actively being processed (but not afterwards).

13. **Merchant's use of Card Data**. You agree not to use or disclose Card Data except for the purposes of obtaining authorisation from the card issuer, completing and settling the Card Transaction for which the Card Data was given to you, together with resolving any Chargeback or Reversal Dispute, or similar issues involving Card Transactions. PayPal is required by banking laws to refund payments lacking the payer's authorisation, so your use of Card Data to carry out a Card Transaction must be authorised by the cardholder or it will subject to Reversal.

14. **Secure storage and disposal of Card Data**. You agree to:
    a. establish and maintain sufficient controls for limiting access to all records containing Card Data;
    b. not sell or disclose to a third party any Card Data or any information obtained in connection with a Card Transaction;
    c. keep no Card Data on paper or in portable digital storage devices such as USB memory devices or removable disks;
    d. not reproduce any electronically captured signature of a cardholder except on PayPal's specific request; and
    e. destroy Card Data either by destroying the medium on which the Card Data are stored or by erasing or rendering the Card Data completely and irreversibly unintelligible and meaningless.

If you transfer your business, Card Data and any information you have about Card Transactions is not transferable under Card Association rules as an asset of the business. In such cases, you agree to provide the Card Data and any transactional data to PayPal if it requests. If PayPal does not request such data, you must destroy it when your business transfers.

15. **PCI DSS audit**. If PayPal so requests, you agree that a Qualified Security Assessor may conduct a security audit of your systems, controls and facilities and issue a report to PayPal and the Associations. You agree to cooperate fully in the conduct of this audit, and to provide any information and access to your systems required by the auditor for the

performance of the audit. You also agree to bear the reasonable expenses of this audit. If you fail to initiate such an audit after PayPal requests you to do so, you authorise PayPal to take such action at the Merchant's expense, or PayPal may immediately suspend your use of your Product. You will receive a copy of the audit report, and PayPal must also receive a copy and provide a copy to any Acquiring Institution or Card Association that requests a copy.

Schedule 2

DATA PROTECTION SCHEDULE

This Data Protection Schedule applies only to the extent that PayPal acts as a processor or Sub-processor to Merchant. Capitalized terms used but not defined in this Schedule shall have the meaning set out in the Agreement.

1 DEFINITIONS AND INTERPRETATION

1.1 The following terms have the following meanings when used in this Schedule:

"**Card Information**" is defined in Section 2.15 of this Schedule.

"**Customer**" means a European Union customer of Merchant who uses the PayPal services and for the purposes of this Schedule is a data subject.

"**Customer Data**" means the personal data that the Customer provides to Merchant and Merchant passes on to PayPal through the use by the Merchant of the PayPal services.

"**data controller**" (or simply "controller") and "data processor" (or simply "processor") and "data subject" have the meanings given to those terms under the Data Protection Laws.

"**Data Protection Laws**" means General Data Protection Regulation (EU) 2016/679 (GDPR) and any associated regulations or instruments and any other data protection laws, regulations, regulatory requirements and codes of conduct of EU Member States applicable to PayPal's provision of the PayPal services.

"**Data Recipient**" is defined in Section 2.15 of this Schedule.

"**PayPal Group**" means PayPal and all companies in which PayPal or its successor directly or indirectly from time to time owns or controls.

"**personal data**" has the meaning given to it in the Data Protection Laws.

"**processing**" has the meaning given to it in the Data Protection Laws and "process", "processes" and "processed" will be interpreted accordingly.

"**Sub-processor**" means any processor engaged by PayPal and/or its affiliates in the processing of personal data.

1.2 **Schedule.** This Schedule comprises (i) sections 1 to 2, being the main body of the Schedule; (ii) Attachment 1; (iii) Attachment 2; and (iv) Attachment 3 (with its appendixes).

2 PROCESSING OF PERSONAL DATA IN CONNECTION WITH THE SERVICES

2.1 **Merchant data controller.** With regard to any Customer Data to be processed by PayPal in connection with this Agreement, Merchant will be a controller and PayPal will be a processor in respect of such processing. Merchant will be solely responsible for determining the purposes for which and the manner in which Customer Data are, or are to be, processed.

2.2 **Merchant written instructions.** PayPal shall only process Customer Data on behalf of and in accordance with Merchant's written instructions. The Parties agree that this Schedule is Merchant's complete and final written instruction to PayPal in relation to Customer Data. Additional instructions outside the scope of this Schedule (if any) require prior written agreement between PayPal and Merchant, including agreement of any additional fees payable by Merchant to PayPal for carrying out such additional instructions. Merchant shall ensure that its instructions comply with all applicable laws, including Data Protection Laws, and that the processing of Customer Data in accordance with Merchant's instructions will not cause PayPal to be in breach of Data Protection Laws. The provisions of this Section are subject to the provisions of Section 2.14 on

Security. Merchant hereby instructs PayPal to process Customer Data for the following purposes:

2.2.1 as reasonably necessary to provide the PayPal services to Merchant and its Customer;

2.2.2 after anonymizing the Customer Data, to use that anonymized Customer Data, directly or indirectly, which is no longer identifiable personal data, for any purpose whatsoever.

2.3 **PayPal cooperation.** In relation to Customer Data processed by PayPal under this Agreement, PayPal shall co-operate with Merchant to the extent reasonably necessary to enable Merchant to adequately discharge its responsibility as a controller under Data Protection Laws, including without limitation as Merchant requires in relation to:

2.3.1. assisting Merchant in the preparation of data protection impact assessments to the extent required of Merchant under Data Protection Laws; and

2.3.2 responding to binding requests from data protection authorities for the disclosure of Customer Data as required by applicable laws.

2.4 **Scope and Details of Customer Data processed by PayPal.** The objective of processing Customer Data by PayPal is the performance of the PayPal services pursuant to the Agreement. PayPal shall process the Customer Data in accordance with the specified duration, purpose, type and categories of data subjects as set out in Attachment 2 (Data Processing of Customer Data).

2.5 **Compliance with Laws.** The Parties will at all times comply with Data Protection Laws.

2.6 **Correction, Blocking and Deletion.** To the extent Merchant, in its use of the PayPal services, does not have the ability to correct, amend, block or delete Customer Data, as required by Data Protection Laws, PayPal shall comply with any commercially reasonable request by Merchant to facilitate such actions to the extent PayPal is legally permitted to do so. To the extent legally permitted, Merchant shall be responsible for any costs arising from PayPal’s provision of such assistance.

2.7 **Data Subject Requests.** PayPal shall, to the extent legally permitted, promptly notify Merchant if it receives a request from a Customer for access to, correction, amendment or deletion of that Customer's personal data. Merchant shall be responsible for responding to all such requests. If legally permitted, PayPal shall provide Merchant with commercially reasonable cooperation and assistance regarding such Customer's request and Merchant shall be responsible for any costs arising from PayPal's assistance.

2.8 **Training.** PayPal undertakes to provide training as necessary from time to time to the PayPal personnel with respect to PayPal's obligations in this Schedule to ensure that the PayPal personnel are aware of and comply with such obligations.

2.9 **Limitation of Access.** PayPal shall ensure that access by PayPal's personnel to Customer Data is limited to those personnel performing PayPal services in accordance with the Agreement.

2.10 **Sub-processors.** Merchant specifically authorizes the engagement of members of the PayPal Group as Sub-processors in connection with the provision of the PayPal services. In addition, Merchant generally authorizes the engagement of any other third parties as Sub-processors in connection with the provision of the PayPal services. When engaging any Sub-processor, PayPal will execute a written contract with the Sub-processor, which contains terms for the protection of Customer Data which are no less protective than the terms set out in this Schedule. PayPal shall make available to Merchant a current list of Sub-processors for the respective PayPal services with the identities of those Sub-processors.

2.11 **Audits and Certifications.** Where requested by Merchant, subject to the confidentiality obligations set forth in the Agreement, PayPal shall make available to Merchant (or Merchant's independent, third-party auditor that is not a competitor of PayPal or any members of PayPal or the PayPal Group) information regarding PayPal's compliance with the obligations set forth in this Schedule in the form of the third-party certifications and audits (if any) set forth in the Privacy Policy set out on our website. Merchant may contact PayPal in accordance with the Agreement to request an on-site audit of the procedures relevant to the protection of personal data. Merchant shall reimburse PayPal for

any time expended for any such on-site audit at PayPal's then-current professional PayPal services rates, which shall be made available to Merchant upon request. Before the commencement of any such on-site audit, Merchant and PayPal shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Merchant shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by PayPal. Merchant shall promptly notify PayPal with information regarding any non-compliance discovered during the course of an audit.

2.12 **Security.** PayPal shall, as a minimum, implement and maintain appropriate technical and organizational measures as described in Attachment 1 to this Schedule to keep Customer Data secure and protect it against unauthorized or unlawful processing and accidental loss, destruction or damage in relation to the provision of the PayPal services. Since PayPal provides the PayPal services to all Merchants uniformly via a hosted, web-based application, all appropriate and then-current technical and organizational measures apply to PayPal's entire customer base hosted out of the same data center and subscribed to the same service. Merchant understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, PayPal is expressly permitted to implement adequate alternative measures as long as the security level of the measures is maintained in relation to the provision of the PayPal services.

2.13 **Security Incident Notification.** If PayPal becomes aware of a Security Incident in connection with the processing of Customer Data, PayPal will, in accordance with Data Protection Laws: (a) notify Merchant of the Security Incident promptly and without undue delay; (b) promptly take reasonable steps to minimize harm and secure Customer Data; (c) describe, to the extent possible, reasonable details of the Security Incident, including steps taken to mitigate the potential risks; and (d) deliver its notification to Merchant's administrators by any means PayPal selects, including via email. Merchant is solely responsible for maintaining accurate contact information and ensuring that any contact information is current and valid.

2.14 **Deletion.** Upon termination or expiry of the Agreement, PayPal will delete or return to Merchant all Customer Data processed on behalf of the Merchant, and

PayPal shall delete existing copies of such Customer Data except where necessary to retain such Customer Data strictly for the purposes of compliance with applicable law.

2.15 **Data Portability.** Upon any termination or expiry of this Agreement, PayPal agrees, upon written request from Merchant, to provide Merchant's new acquiring bank or payment service provider ("Data Recipient") with any available credit card information including personal data relating to Merchant's Customers ("Card Information"). In order to do so, Merchant must provide PayPal with all requested information including proof that the Data Recipient is in compliance with the Association PCI-DSS Requirements and is level 1 PCI compliant. PayPal agrees to transfer the Card Information to the Data Recipient so long as the following applies: (a) Merchant provides PayPal with proof that the Data Recipient is in compliance with the Association PCI-DSS Requirements (Level 1 PCI compliant) by providing PayPal a certificate or report on compliance with the Association PCI-DSS Requirements from a qualified provider and any other information reasonably requested by PayPal; (b) the transfer of such Card Information is compliant with the latest version of the Association PCI-DSS Requirements; and (c) the transfer of such Card Information is allowed under the applicable Association Rules, and any applicable laws, rules or regulations (including Data Protection Laws).

3 EU STANDARD CONTRACTUAL CLAUSES RELATED TERMS

3.1 **Application.** The EU Standard Contractual Clauses are set out in Attachment 3 (the "EU Standard Contractual Clauses"). The EU Standard Contractual Clauses apply only to Customer Data that is transferred by Merchants established in the European Economic Area ("EEA") or Switzerland to any country outside the EEA that is not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR) in which PayPal may store and process Customer Data.

3.2 **Instructions.** This Schedule and the Agreement are Data Exporter's complete and final instructions to Data Importer for the processing of Customer Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the EU Standard Contractual Clauses, the Data Exporter gives the following instructions: (a) to process Customer Data in

accordance with the Agreement; and (b) to process Customer Data initiated by Merchants in their use of the Services during the Term. These instructions also describe the duration, object, scope and purpose of the processing.

3.3 **Audits and Certifications.** The Parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the EU Standard Contractual Clauses shall be fulfilled in the following manner: the provisions of paragraph 2.11 of this Schedule shall also apply to the Data Importer as if it were PayPal.

3.4 **Certification of Deletion.** The Parties agree that the certification of deletion of personal data that is described in Clause 12(1) shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's request.

3.5 **Liability.** The Parties agree that all liabilities between them (and in respect of Data Importer, such liabilities shall be aggregated with those of PayPal so that collectively their cumulative joint liability is capped at the level set out in the Agreement) under this Schedule and the EU Standard Contractual Clauses will be subject to the terms of the Agreement (including as to limitation of liability), except that such limitations of liability will not apply to any liability that Data Importer may have to data subjects under the third party rights provisions of the EU Standard Contractual Clauses.

3.6 **Exclusion of third party rights.** Subject to paragraph 4.6, PayPal shall be granted third party rights in relation to obligations expressed to be for the benefit of the Data Importer or PayPal in this Schedule and Data Subjects are granted third party rights under the EU Standard Contractual Clauses. All other third party rights are excluded.

Merchant
For and on behalf of (insert Merchant legal name)……
Signature……
Name of signatory……. Title of signatory……
Date……..

PayPal
For and on behalf of PayPal (Europe) S.á.r.l. et Cie, S.C.A.
Signature…….

Name of signatory……..Title of signatory…….
Date……

ATTACHMENT 1
Technical and Organizational Measures

The following technical and organizational measures will be implemented:

1. Measures taken to prevent any unauthorized person from accessing the facilities used for data processing;
2. Measures taken to prevent data media from being read, copied, amended or moved by any unauthorized persons;
3. Measures taken to prevent the unauthorized introduction of any data into the information system, as well as any unauthorized knowledge, amendment or deletion of the recorded data;
4. Measures taken to prevent data processing systems from being used by unauthorized person using data transmission facilities;
5. Measures taken to guarantee that authorized persons when using an automated data processing system may access only data that are within their competence;
6. Measures taken to guarantee the checking and recording of the identity of third parties to whom the data can be transmitted by transmission facilities;
7. Measures taken to guarantee that the identity of the persons having had access to the information system and the data introduced into the system can be checked and recorded ex post facto at any time and by any authorized person;
8. Measures taken to prevent data from being read, copied, amended or deleted in an unauthorized manner when data are disclosed and data media transported;
9. Measures taken to safeguard data by creating backup copies.

ATTACHMENT 2
Data Processing of Customer Data

Categories of data subjects

Customer Data – The personal data that the Customer provides to Merchant and Merchant passes on to PayPal through the use by the Customer of the PayPal services.

Subject-matter of the processing

The payment processing services offered by PayPal which provides Merchant with the ability to accept credit cards, debit cards, and other payment methods on a website or mobile application from Customers.

Nature and purpose of the processing

PayPal processes Customer Data that is sent by the Merchant to PayPal for purposes of obtaining verification or authorization of the Customer's payment method as payment to the Merchant for the sale goods or services.

Type of personal data

Customer Data – Merchant shall inform PayPal of the type of Customer Data PayPal is required to process under this Agreement. Should there be any changes to the type of Customer Data PayPal is required to process then Merchant shall notify PayPal immediately. PayPal processes the following Customer Data, as may be provided by the Merchant to PayPal from time to time:

	Payment Pro	Virtual Terminal	Payments Pro Payflow	Payments Ad
Full name	X	X	X	X
Shipping address	X	X	X	X
A Billing address	X	X	X	X
Email address	X	X	X	X
Telephone number	X	X	X	X
Fax number			X	
Government ID number			X	
Bank account and Bank routing number			X	
Card or payment instrument type (optional)	X	X	X	X
Card Primary Account Number (PAN)	X	X	X	X
Card Verification Value (CVV)	X	X	X	X
Card expiration date	X	X	X	X
Business Tax ID			X	
IP address	X		X	

Special categories of data (if relevant)

The transfer of special categories of data is not anticipated.

Duration of Processing

The term of the Agreement.

ATTACHMENT 3
EU STANDARD CONTRACTUAL CLAUSES

Controller to Processor export of personal data (from EEA countries)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection
Name of the data exporting organisation: ……..
Address: …….
Tel.: …….
fax: ……..
e-mail: ……..
Other information needed to identify the organisation: ……
(the data exporter)
And
Name of the data importing organisation: Paypal, Inc
Address: 2211 North First Street, San Jose, CA 95131
Other information needed to identify the organisation: ……
(the data importer)
each a “party”; together “the parties”,
HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) 'the data exporter' means the controller who transfers the personal data;
- (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:

    o (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
    o (ii) any accidental or unauthorised access, and
    o (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law
The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract
The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer

warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full): …….
Position: …….
Address: …….
Other information necessary in order for the contract to be binding (if any):
Signature…….(stamp of organisation)

On behalf of the data importer (Paypal, Inc):
Name (written out in full): …….
Position: ……..
Address: 2211 North First Street, San Jose, CA 95131
Signature……. (stamp of organisation)

APPENDIX 1 TO THE EU STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is: Merchant

An entity that uses the Data importer's services in respect of its Customers

Data importer

The data importer is: Paypal, Inc

A payment services provider which in relation to the Braintree services provides a payment gateway so that Merchant can provide Customer credit card and other details to banks and other payment service providers to process payments from Customers

Data subjects

The personal data transferred concern the following categories of data subjects:
The data exporter's Customers

Categories of data

The personal data transferred concern the following categories of data:
Customer name, amount to be charged, card number, CSV, post code, country code, address, email address, fax, phone, website, expiry date, shipping details, tax status

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):
Not applicable, unless Merchant configures the service to capture such data.

Processing operations

The personal data transferred will be subject to the following basic processing activities:
The receipt and storage of Personal Data in the performance of the Services during the Term of the Agreement.

APPENDIX 2 TO THE EU STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c)

(or document/legislation attached):

The technical and organizational measures are set forth at Attachment 1 to this Amendment.

Back to top

#oct9

>> View all legal agreements

PayPal Website Payments Pro and Virtual Terminal Agreement

Last Update: June 09, 2016

Print Download PDF

Please note: The version of this Agreement marked "Current PayPal Website Payments Pro and Virtual Terminal Agreement" set out immediately below is effective until January 9, 2018. The version of this Agreement marked "Updated PayPal Website Payments Pro and Virtual Terminal Agreement" further below will take effect and supersede the Current PayPal Website Payments Pro and Virtual Terminal Agreement on January 9, 2018.

Current PayPal Website Payments Pro and Virtual Terminal Agreement

This PayPal Website Payments Pro / Virtual Terminal Agreement ("Agreement") is a contract between you (also referred to as the "Merchant") and PayPal (Europe) S.àr.l. et Cie, S.C.A. ("PayPal" or "we"). You agree that any use by you

of Online Card Payment Services shall constitute your acceptance of this Agreement and we recommend that you store or print-off a copy of this Agreement. PayPal is licensed as a Luxembourg credit institution and is under the prudential supervision of the Luxembourg supervisory authority, the Commission de Surveillance du Secteur Financier (the "CSSF"). The CSSF has its registered office in L-1150 Luxembourg. Because the funds in your PayPal Account are electronic money, which does not legally qualify as a deposit or an investment service, you are not protected by the Luxembourg deposit guarantee schemes provided by the Association pour la Garantie des Dépôts Luxembourg.

This Agreement applies to your use of PayPal Website Payments Pro and/or Virtual Terminal (the "Products"). To proceed with obtaining one or both of the Products, you must read, agree with and accept all of the terms and conditions contained in this Agreement.

We may make Changes to this Agreement by giving notice of such Change by posting a revised version of this Agreement on the PayPal website(s). A Change will be made unilaterally by us and you will be deemed to have accepted the Change after you have received notice of it. We will give you 2 months' notice of any Change with the Change taking effect once the 2 month notice period has passed, except the 2 month notice period will not apply where a Change relates to the addition of a new service, extra functionality to the existing Service or any other change which neither reduces your rights nor increases your responsibilities. In such instances, the change will be made without notice to you and shall be effective immediately upon giving notice of it. All future Changes set out in the **Policy Update** already published on the “Legal Agreements” landing page of the PayPal website at the time you register for the Online Card Payment Services are incorporated by reference into this Agreement and will take effect as specified in that **Policy Update**.

If you do not accept any Change, you must close your Account following the account closure procedure set out in the User Agreement. If you do not object to a Change by closing your Account within the 2 month notice period, you will be deemed to have accepted the Change. While you may close your Account at any time and without charge, please note that you may still be liable to us after you terminate this Agreement for any liabilities you may have incurred and are

responsible for prior to terminating this Agreement and please further note our rights under the User Agreement.

Capitalised terms are defined below. Please view **download and save** this agreement.

1. Setting up and activating your Product

1. **Getting started.** To obtain and use your Product, you must first do all of the following:
    a. Complete the online application and approval process for your Product, open a PayPal Business Account (if you do not already have one), and follow the instructions set out in PayPal's online process to access and use your Product.
    b. Integrate your Product into the payment process of your website, if your Product is Website Payments Pro. You are not required to integrate your Product into the payment process of your website if you only access and use Virtual Terminal. PayPal is not responsible for any problems that could occur by integrating your Product into your 'live' website.
    c. Activate your Product by using it in a 'live' payment transaction for the first time.

    If your Product is Website Payments Pro, you may only integrate and use Website Payments Pro in one of the following mutually exclusive ways - either (i) as a PayPal Hosted Solution (in which PayPal operates Website Payments Pro for you as a PayPal-hosted service) or (ii) operated on your own facilities - (each option being a **"Hosting Option")**. PayPal may (but, notwithstanding any other provision in this Agreement, shall not be obliged to) provide both Hosting Options. PayPal may, at its sole discretion, set either Hosting Option as your default option for integrating the Direct Payments API into the payment process of your website.

2. **Required use of Express Checkout.** If your Product is Website Payments Pro, you must implement PayPal Express Checkout as part of your website integration; see clause 2(1) below. In implementing Express Checkout, you agree that your website:
    a. Includes a PayPal Express Checkout button either: (A) before you request the shipping/billing address and other financial information

from your customers or (B) on the same page that you collect such information if you only use one page for your checkout process.

b. Offers PayPal as a payment option together with the other payment options you offer for Express Checkout. The PayPal logo must be displayed with equal or greater prominence as the logos for your other payment options.
c. Provides your customers with the option of not storing their personal information, including their email address, shipping/billing address, and financial information, as part of the checkout process.

Failure to implement Express Checkout affects the fees you pay; see clause 2(1) and 2(3).

3. **Your information.** You confirm that you have read, consented and agreed to PayPal's Privacy Policy, which explains the information that we collect about you and your online business. In particular, you agree and consent that PayPal may obtain from a third party your credit history and financial information about your ability to perform your obligations under this Agreement; the PayPal Privacy Policy lists the companies involved in this exchange of credit-related information. PayPal will review your credit and other risk factors of your Account (reversals and chargebacks, customer complaints, claims etc.) on an ongoing basis, and we may also review your website and the products for sale on it. PayPal will store, use and disclose all information that we have about you in conformity with PayPal's Privacy Policy.

5. **Cancellation.** PayPal may terminate your access to and/or use of either or both Products and / or terminate this Agreement at any time before the Activation Date by notifying you.

2. Fees

1. **How fees are paid**. You agree to pay the fees in this Agreement as they become due without set-off or deduction. You authorise PayPal to (and PayPal may) collect Monthly Fees first from any available Balance in your Account and then also from the funding source(s) registered for your Account, and you authorise PayPal to (and PayPal may) collect fees for receiving payments from the payments you receive before those funds are credited to your account. If PayPal is unable to collect a past due fee from your Account and its funding source(s), we may take action against you as provided in the User Agreement for unpaid fees.

Except as further provided in this Agreement, you agree to pay the fees set out in the User Agreement.

Fees will be charged in the currency of the payment received.

See the Glossary at clause 2.6 for further reference.

2. **Monthly Fees**

Product	**Monthly Fee**
Website Payments Pro (including Express Checkout, Direct Payments API, Virtual Terminal and Fraud Management Filters)	GBP 20.00
Virtual Terminal only	GBP 20.00

3.

3. **Transaction Fees for Standard PayPal Payments with Express Checkout**

If you receive the payment:	**the PayPal Standard Rate fee is:**	**the PayPal Merchant Rate is as follows:**	
		where the aggregate monetary amount of payments received in your PayPal Account in the previous calendar month is:	**the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:**
as a Standard PayPal Payment using Express Checkout	3.4% + Fixed Fee	GBP 0.00 - GBP 1,500.00	3.4% + Fixed Fee
		GBP 1,500.01 - GBP 6,000.00	2.9% + Fixed Fee
		GBP 6,000.01 - GBP 15,000.00	2.4% + Fixed Fee

		GBP 15,000.01 – GBP 55,000.00	1.9 % + Fixed Fee
		Above GBP 55,000.00	1.4 % + Fixed Fee

4.

4. **Transaction Fees for Card Payments under the Blended Pricing Fee Structure**

If you receive a payment:	**the PayPal Standard Rate fee is:**	**the PayPal Merchant Rate is as follows:**	
		where the aggregate monetary amount of payments received in your PayPal Account in the previous calendar month is:	**the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:**
from a card (Visa, MasterCard or Maestro) using the Online Card Payment Services	3.4% + Fixed Fee	GBP 0.00 - GBP 1,500.00	3.4% + Fixed Fee
		GBP 1,500.01 - GBP 6,000.00	2.9% + Fixed Fee
		GBP 6,000.01 - GBP 15,000.00	2.4% + Fixed Fee
		Above GBP 15,000.00	1.9 % + Fixed Fee

5.

5. **Transaction Fees for Card Payments under the Interchange Plus Fee Structure**

		the PayPal Merchant Rate is as follows:

If you receive a payment:	the PayPal Standard Rate fee is:	where the aggregate monetary amount of payments received in your Account in the previous calendar month is:	the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:
from a card (Visa, MasterCard or Maestro) using the Online Card Payment Services	Interchange Fee (approximately ranges from 0.2% to 2.0%) + 2.9% + Fixed Fee	GBP 0.00 - GBP 1,500.00	Interchange Fee + 2.9% + Fixed Fee
		GBP 1,500.01 - GBP 6,000.00	Interchange Fee + 2.4% + Fixed Fee
		GBP 6,000.01 - GBP 15,000.00	Interchange Fee + 1.9% + Fixed Fee
		Above GBP 15,000.00	Interchange Fee + 1.4% + Fixed Fee

6.

6. **Glossary**

a. Interchange Fees are set by Visa and MasterCard. They approximately range from 0.2% to 2.0% and vary for different types of cards (for example by categories and brand). **PayPal shall always charge you the Interchange Fee as set by Visa and MasterCard and as passed on by its Acquirer.** Single Interchange fees may change from time to time. For more information on Interchange Fees, please see **MasterCard's** and **Visa's**website as well as our **simplified overview**.

b. Percentage-based fees (such as 3.4%) refer to an amount equal to that percentage of the payment amount.

c. Fixed Fees are based on the currency received, as follows:

Argentine Peso:	2.00 ARS	New Zealand Dollar:	$0.45 NZD
Australian Dollar:	$0.30 AUD	Norwegian Krone:	2.80 NOK
Brazilian Real:	0.60 BRL	Philippine Peso:	15.00 PHP
Canadian Dollar:	$0.30 CAD	Polish Zloty:	1.35 PLN
Czech Koruna:	10.00 CZK	Russian Ruble	10.00 RUB
Euro:	€0.35 EUR	Singapore Dollar:	0.50 SGD
Danish Kroner:	2.60 DKK	Swedish Kronor:	3.25 SEK
Hong Kong Dollar:	$2.35 HKD	Swiss Franc:	0.55 CHF
Hungarian Forint:	90 HUF	Taiwan New Dollar:	10.00 TWD
Israeli New Shekels:	1.20 ILS	Thai Baht:	11.00 THB
Japanese Yen:	¥40 JPY	Turkish Lira:	0.45 TRY
Malaysian Ringgit:	2 MYR	**UK Pounds Sterling:**	**£0.20 GBP**
Mexican Peso:	4.00 MXN	US Dollar:	$0.30 USD

7.

7. **Blended Pricing or Interchange Plus Transaction Fees?**

   When you receive card payments using any of our Online Card Payment Services (including via Direct Payment API or Virtual Terminal):

   a. The Blended Pricing fee structure shall apply until PayPal implements the Interchange Plus fee structure (which shall be by further notice of the same published by PayPal on a date falling on or after 9 June 2016 on the Policy Updates page accessible via the Legal footer on most PayPal site pages) ("**Interchange Plus Launch**").
   b. You may choose the fee structure applicable to you on or after Interchange Plus Launch, by the methods or procedures that PayPal may make available to you before and after Interchange Plus Launch. If you do not make an election, you will stay on your existing fee structure.
   c. You may choose your fee structure for future transactions only, not for past transactions. The fee structure that applies when you receive card payments using any of our Online Card Payment Services also applies when you receive card payments using PayPal

Here™. This means that if you opt to be charged under the Interchange Plus fee structure, the respective Interchange Plus fee structure will apply to the use of both our Online Card Payment Services and PayPal Here.

8. **Merchant Rate**

Merchant Rate applies only to Accounts with Merchant Rate status. Merchant Rate status is subject to eligibility, application and approval by PayPal. PayPal may evaluate applications on a case-by-case basis, including, without limitation, on the following criteria: qualifying monthly sales volume, size of average shopping cart and an Account in good standing. To be eligible to apply for (and retain) PayPal Merchant Rate status the Account must:

- at all times be in good standing and not under investigation; and
- have received more than £1,500.00 GBP in aggregate monetary amount of payments in the previous calendar month.

PayPal may downgrade an Account to the Standard Rate at any time if the above conditions are not met or there are unresolved chargebacks against the Account.

If PayPal downgrades your Account you will need to apply to PayPal again for your Account to get Merchant Rate status.

You may apply to receive Merchant Rate for your Account using the dedicated online **application form** when logged into your PayPal Account. If your application is rejected, please note that you may only submit an application once every thirty days.

9. **Additional Transaction Fees**

a. Receiving Cross Border Payments

When you receive a Cross Border payment (which for the purpose of this Agreement also includes any payment made by a card from outside the United Kingdom) you agree to pay an additional percentage-based Cross Border Fee as set out in the table below (depending on the sender's country).

Sender's country	Cross Border Fee

Northern Europe*	0.4%
Europe I**	0.5%
US / Canada	1.0%
Europe II***	1.3%
Rest of World	1.8%

10. * Aland Islands, Denmark, Faroe Islands, Finland, Greenland, Iceland, Norway, Sweden.

    ** Austria, Belgium, Channel Islands, Cyprus, Estonia, France (including French Guiana, Guadeloupe, Martinique, Reunion and Mayotte), Germany , Gibraltar, Greece, Ireland, Isle of Man, Italy , Luxembourg, Malta, Monaco, Montenegro, Netherlands, Portugal, San Marino, Slovakia, Slovenia, Spain, United Kingdom, Vatican City State.

11. *** Andorra, Albania, Belarus, Bosnia & Herzegovina, Bulgaria, Croatia, Czech Republic, Georgia, Hungary, Kosovo, Latvia, Liechtenstein, Lithuania, Macedonia, Moldova, Poland, Romania, Russian Federation, Serbia, Switzerland, Turkey, Ukraine.

12. This fee does not apply to:

    - Cross Border Euro or Swedish Krona payments made (i) between Accounts registered in; or (ii) by cards from the European Union or EEA do not incur this additional fee.
    - payments received from **cards using the Online Card Payment Services under the Interchange Plus fee structure**.

    b. Failure to implement Express Checkout. If you do not implement Express Checkout as required in clause 1 (2) above, the percentage components of the Transaction Fees set out in clause 2.2 will each increase by an additional 0.5 % after PayPal gives you 30 days' notice. You agree to pay the increased fees.

    c. Additional risk factors. If PayPal determines that your Account receives, or is likely to receive, a disproportionately high number of customer complaints, Reversals, Chargebacks, Claims, or other indicators

of a serious level of risk, PayPal may increase the percentage components of your Transaction Fees by up to 5%, after giving you 30 days prior notice of the increase. You agree to terminate your use of the Product if you do not agree to this increase.

10. **Other Fees**

Activity/Event/Product	Fee
. **Recurring Payment Tool (optional service)**	GBP 20.00 per month
b. **Uncaptured Authorisation Transactions**	GBP 0.20 for each successful but uncaptured authorisation transaction via Direct Payment API or Virtual Terminal
c. **Card Account Verification Transactions**	0.20 GBP for each card account verification request (for all Direct Payment API or Virtual Terminal card account verification transactions (Visa and MasterCard only). For the avoidance of doubt, this does not include Uncaptured Authorisation Transactions.

11. **MasterCard transactions**. For further information about MasterCard's rules and rates, please visit: **http://www.mastercard.com/us/merchant/index.html**.

12. **Monthly Reports on Transaction Costs**. PayPal shall make available monthly reports on transaction costs (inclusive of interchange fees) for card transactions which you process with PayPal Website Payments Pro and Virtual Terminal. These reports will be downloadable from your PayPal Account. The reports do not include any Standard PayPal payments.

3. Settlement of Card Payments within the Interchange Plus Fee Structure

You agree that, when PayPal receives a card payment for you, PayPal may hold those funds in your Reserve Account and you are thereby giving a Payment Order that instructs PayPal to pay those funds to your Payment Account only on the Business Day on which PayPal receives the information about the interchange fee applicable to the card payment, at which time the funds will then be made available to you in your Payment Account. While the funds are held in your Reserve Account, the transaction will appear to you as “Pending” in your Account details. PayPal does not consider that the proceeds of the card payment in your Reserve Account are at your disposal until PayPal has received the information on the applicable interchange fee from our Processor (which can be within the next Business Day following the day on which the card payment was initiated by the card holder).

4. Information security

1. **Compliance with Data Security Schedule**. You agree (as a "Merchant") to comply with Schedule 1 below, which forms part of this Agreement.
2. **Your PCI DSS compliance**. You also agree to comply with the PCI Data Security Standard (PCI DSS). You must protect all Card Data that comes within your control according to PCI DSS, and you must design, maintain and operate your website and other systems in conformity with PCI DSS. You must ensure that your staff are and remain sufficiently trained so that they are aware of PCI DSS and can carry out its requirements. PayPal is not responsible for any costs that you incur in complying with PCI DSS.
3. **PayPal’s PCI DSS compliance**. PayPal warrants that PayPal and your Product comply and will comply with PCI DSS. However, PayPal’s compliance, and your Product’s, are not sufficient to achieve compliance with PCI DSS by you and your systems and processes.
4. **3D Secure**. Requirements of the European Central Bank and PayPal’s bank regulators require use of 3D Secure in certain circumstances, and Card Associations may also require it to reduce an excessive number of Card Transactions unauthorised by the cardholder. PayPal may by notice to you require that you implement 3D Secure for all or certain specified Card Transactions. You agree to implement 3D Secure if required in such a notice, where the issuer of a particular card supports 3D Secure for that card.
5. **Price and currency**. You may not submit payment transactions in which the amount is the result of dynamic currency conversion. This means that you may not list an item in one currency and then accept payment in a

different currency. If you are accepting payments in more than one currency, you must separately list the price for each currency.

5. User Agreement

1. **User Agreement applies**. You acknowledge and agree that the User Agreement, and not this Agreement, is the “framework contract” between you and PayPal as defined in laws transposing the Payment Services Directive (2007/64/EC)(. The terms of the User Agreement also apply to you and are incorporated by reference into this Agreement. The definition of “Services” in the User Agreement shall be amended to include your Product, and the definition of “Agreement” shall include this Agreement. In case of any inconsistency between this Agreement and the User Agreement, this Agreement supersedes the User Agreement, but only to the extent of that inconsistency. Where this Agreement and the User Agreement both specify a fee for the same action, the fee specified in this Agreement will apply rather than the fee in the User Agreement. The User Agreement can be found via a link in the footer of nearly every PayPal web page. The User Agreement includes important provisions which:
    a. Permit PayPal to take a Reserve to secure your obligation to pay Chargebacks, Reversals and fees;
    b. Obligate you to follow PayPal’s Acceptable Use Policy in your use of PayPal;
    c. Give legal effect to PayPal’s Privacy Policy, which governs our use and disclosure of your information and that of Shared Customers; and
    d. Permit PayPal to restrict a payment or your PayPal Account in circumstances listed in the User Agreement.
2. **Failed payments and Product tools**. You are responsible for Chargebacks, Reversals and other invalidated payments as provided in the User Agreement, regardless of how you use and configure your Product, including its fraud filtering technology and similar preventive tools (if any). Those tools can be useful in detecting fraud and avoiding payment failures, but they do not affect your responsibility and liability pursuant to the User Agreement for Chargebacks, Reversals and payments which are otherwise invalidated.

6. Intellectual property and ID codes

1. **Licence**. PayPal hereby grants to you a non-exclusive, non-transferable, revocable, non-sublicenseable, limited license to (a) use your Product in

accordance with the documentation provided on the PayPal Website; and to (b) use the documentation provided by PayPal for your Product and reproduce it for internal use only within your business. Your Product as licensed is subject to change and will evolve along with the rest of the PayPal system; see clause 8(1). You must comply with the implementation and use requirements contained in all PayPal documentation and instructions accompanying the Product issued by PayPal from time to time (including, without limitation, any implementation and use requirements we impose on you to comply with applicable laws and card scheme rules and regulations).

2. **ID codes**. PayPal will provide you with certain identifying codes specific to you. The codes identify you and authenticate your messages and instructions to us, including operational instructions to PayPal software interfaces. Use of the codes may be necessary for the PayPal system to process instructions from you (or your website). You must keep the codes safe and protect them from disclosure to parties whom you have not authorised to act on your behalf in dealing with PayPal. You agree to follow reasonable safeguards advised by PayPal from time to time in order to protect the security of those identifying codes. If you fail to protect the security of the codes as advised, you must notify PayPal as soon as possible, so that PayPal can cancel and re-issue the codes. PayPal may also cancel and re-issue the codes if it has reason to believe that their security has been compromised, and after notifying you whenever notice can reasonably be given.
3. **Ownership of PayPal Website Payments Pro information and materials**. As part of Merchant's access to, and utilisation of PayPal Website Payments Pro, Merchant will be provided with certain information and materials (the "Pro Materials") which are able to be used by Merchant to use PayPal Website Payments Pro. All intellectual property rights associated with the Pro Materials remain the property of PayPal or the relevant Acquiring Institution(as the case may be). Merchant agrees to not give, transfer, assign, novate, sell, resell (either partly or in whole) the Pro Materials to any person.

7. Banking terms for Card Transactions

1. PayPal utilises services from banking partners in processing Card Transactions, including both direct payments to you from a card as well as Card Transactions that fund a PayPal payment to you. The **Commercial Entity Agreements** apply in relation to those services. In accepting this Agreement, you also accept the **Commercial Entity Agreements**, which

form part of this Agreement. A copy of the Commercial Entity Agreements can be obtained from the Legal link at the bottom of a PayPal web page.

8. Termination and suspension

1. **By you**. You may terminate this Agreement by doing either of the following:
    a. Giving 10 days' notice to PayPal Customer Service on of your intent to terminate this Agreement. PayPal Customer Service will confirm termination via email. This option lets you stop using your Product and paying for it, but your PayPal Account remains open and its User Agreement remains in effect.
    b. Closing the PayPal Account that you use with your Product (see the User Agreement for more information).
2. **By PayPal**. PayPal may terminate this Agreement by doing any of the following:
    a. Giving you 2 months' notice by email to you at your registered email address associated with your Account of PayPal's intent to terminate this Agreement. Unless otherwise notified, terminating this Agreement does not affect your User Agreement and your PayPal Account remains open.
    b. Terminating the User Agreement that applies to the PayPal Account used with your Product.
3. **By events**. PayPal may terminate this Agreement immediately without notice if you:
    a. Breach this Agreement or the User Agreement;
    b. Become unable to pay or perform your obligations as they fall due;
    c. Become unable to pay your debts (within the meaning of section 123 of the Insolvency Act 1986), admit your inability to pay your debts or otherwise become insolvent;
    d. Have any distraint, execution, attachment or similar action taken, levied or enforced against you or your assets, or if any garnishee order is issued or served on you;
    e. Become the subject of any petition presented, order made or resolution passed for the liquidation, administration, bankruptcy or dissolution of all or a substantial part of your business, except where solvent amalgamation or reorganisation is proposed on terms previously approved by PayPal,
    f. Lose full and unrestricted control over all or part of your assets because of the appointment of a receiver, manager, trustee, liquidator or similar officer;

g. Enter into or proposes any composition or arrangement concerning your debts with your creditors (or any class of its creditors);
h. A material adverse change occurs in your business, operations, or financial condition; or
i. You provide inaccurate information in applying for your Product or in your dealings with us.

4. **Effect of termination**. When this Agreement terminates, you must immediately stop using your Product, and PayPal may prevent or hinder you from using it after termination. If you nevertheless use a Product after termination of this Agreement, then this Agreement will continue to apply to your use of that Product until you give effect to the termination by stopping your use of that Product. The following clauses in this Agreement shall survive termination of this agreement and continue in full force and effect: Clauses 2, 4(1) 8(2), 8(4). Termination of this agreement shall not affect any rights, remedies or obligations of the parties that have accrued or become due prior to termination, and you will not be entitled to a refund of any Monthly Fee paid prior to termination.
5. **Breach and suspension**. If you breach this Agreement, the User Agreement, or a security requirement imposed by PCI DSS, PayPal may immediately suspend your use of your Product (in other words, we may render your Product temporarily inoperable). PayPal may require you to take specified corrective actions to cure the breach and have the suspension lifted, although nothing in this Agreement precludes PayPal from pursuing any other remedies it may have for breach. In addition, if PayPal reasonably suspects that you may be in breach of this Agreement or PCI DSS, PayPal may suspend your use of your Product pending further investigation.

   If PayPal suspends your access to or use of PayPal Website Payments Pro, PayPal will notify you and explain the basis of PayPal's actions in suspending your use of your Product, and may specify corrective actions to cure the breach and have the suspension lifted. PayPal's suspension of the Merchant's access or use of PayPal Website Payments Pro will remain in effect and until such time as PayPal is satisfied that the Merchant has remedied the applicable breach(es).

9. Miscellaneous

1. **Future of the Products**. PayPal retains sole and absolute discretion in determining (a) the future course and development of the Products, (b) which improvements to make in them and when, and (c) whether and when defects are to be corrected and new features introduced. PayPal

welcomes feedback from users in planning the future of the Products but is not required to act in accordance with any feedback received. In giving us feedback, you agree to claim no intellectual property interest in your feedback.

2. **No warranty**. Your Product and all accompanying documentation are provided to you on an "as is" basis. PayPal does not give or offer any warranty, express or implied, by operation of law or otherwise, in relation to your Product, the licensed software or user documentation provided. Nothing provided by PayPal under this Agreement or otherwise for your Product has PayPal's authorisation to include a warranty, and no obligation or liability will arise out of PayPal's rendering of technical, programming or other advice or service in connection with any Product, licensed software and user document provided (including, without limitation, services that may assist you with the customisation of your Product). PayPal recommends that you test the implementation of your Product thoroughly as PayPal is not responsible for any loss caused by a defect in it.

   If PayPal hosts your Product (in other words, we run the software for you as a web service), PayPal does not guarantee continuous, uninterrupted or secure access to your hosted Product. PayPal will not be liable for any delay or failure in hosting your Product. You acknowledge the availability of your Product for use may be occasionally limited to allow for repairs, maintenance or the introduction of new facilities or services.

3. **Indemnity**. You agree to indemnify PayPal and keep PayPal fully indemnified on a continuing basis from any direct loss, damage and liability, and from any claim, demand or cost (including reasonable attorneys' fees) incurred in relation to any third party (including a Shared Customer) and arising out of your breach of this Agreement, the User Agreement and the documents incorporated in it by reference (including the Acceptable Use Policy), or the violation of any law.

4. **PayPal Hosted Solution and your intellectual property**. You hereby grant to PayPal a royalty-free, worldwide non-exclusive licence to use your or any of your affiliates' names, images, logos, trademarks, service marks, and/or trade names as you may provide to PayPal when using the Products ("Your Marks") for the sole purpose of enabling your use of the Products (including, without limitation, the customisation of your hosted Product). Title to and ownership of Your Marks and all goodwill arising from any use hereunder will remain with you. You represent and warrant that you have the authority to grant PayPal the right to use Your Marks and you shall indemnify PayPal and keep PayPal fully indemnified on a

continuing basis from any claims or losses suffered by it arising from the use of Your Marks in connection with the Products.

5. **Assignment, amendment and waiver**. You may not assign this Agreement without first obtaining PayPal's written consent. PayPal may assign, novate or otherwise transfer this agreement without your consent by notifying you. Neither party may amend this Agreement or waive any rights under it except in a written document signed by both parties.

6. **English law and jurisdiction**. This Agreement is governed by English law. The parties submit to the non-exclusive jurisdiction of the courts of England and Wales.

10. Definitions

Capitalised terms not listed in this clause are defined in the User Agreement.

1. **3D Secure**: A security procedure that enables a card-issuing bank to authenticate the cardholder authorising a Card Transaction at the time a payment is made. 3D Secure has other brand names depending on the Card Association whose branding appears on the card; brand names for 3D Secure include Verified by Visa and MasterCard SecureCode.
2. **Account Nationality**: The "Account Nationality" of a PayPal Account is the same as that of the bank account into which PayPal E-money is withdrawn (redeemed). For example, if a Spanish bank account is registered as the account into which PayPal E-money is withdrawn, then the Account Nationality of the PayPal Account from which that redemption occurs is Spanish. A PayPal Account from which E-money is withdrawn into a German bank account would be German, even though a German and Spanish Account would both be denominated in the same currency (Euros).
3. **Acquiring Institution:** means a financial institution or bank that provides services to you and PayPal to enable you to (a) accept payment by cardholders using cards: and (b) receive value in respect of Card Transactions.
4. **Activation Date**: The date on which you complete all of the steps for "Getting started" as listed in clause 1(1) above.
5. **Advanced Fraud Management Filters** : Technology provided by PayPal to enable you to (a) check a card payment against criteria such as the cardholder's billing address (Address Verification Service or AVS), the card's CVV2 Data, and databases of suspicious addresses, identifiers, and patterns. See the PayPal Website and product documentation for further

information. Advanced Fraud Management Filters offer a greater level of transaction screening, and transactions can be automatically flagged, reviewed or declined based on how you configure the filters.

6. **AVS Data**: Information returned by the Address Verification System operated by or on behalf of Card Associations, which compares address data provided by an apparent cardholder with address data on file for the card at the card issuer.
7. **Card Association**: A company or consortium of financial institutions which promulgates rules to govern Card Transactions that involve the card that carries the company's or the consortium's brand. Examples include Visa USA, Visa Europe, and the other Visa regions; Mastercard International Incorporated; American Express Company and similar organisations.
8. **Card Data**: All personal or financial information relevant to a Card Transaction, including information recorded on the card itself (whether in human-readable form or digitally), together with the cardholder's name and address and any other information necessary for processing a Card Transaction.
9. **Card Transaction**: A payment made using a credit or debit card, an American Express card, or any other payment method using a physical data-carrying item intended to be held in the payer's possession. The Products support only certain types of Card Transactions; see the PayPal Website for more information.
10. **Critical Systems**: The information technology (both hardware and software) that you employ to operate your Products, to protect them and your online points of sale against intrusion and interference, and to store payment-related and personal data, including any Card Data that you retain and all personal data about Shared Customers.
11. **CVV2 Data**: The three-digit number printed to the right of the card number in the signature panel area on the back of the card. (For American Express cards, the code is a four-digit unembossed number printed above the card number on the front of the American Express card.) The CVV2 Data are uniquely associated with each individual plastic card and ties the card account number to the plastic.
12. **Data Breach**: An intrusion into or malfunction of a computer system in which Card Data are stored, and which intrusion or malfunction either (a) exposes, modifies or destroys all or part of the Card Data in the system, or (b) runs a significant risk, in the opinion of a qualified expert in information security, of exposing, modifying or destroying all or part of the Card Data in the system. Card Data are exposed where they are released from the normal access controls of the system without authorisation, or where they are actually disclosed to one or more unauthorised persons.
13. **Data Protection Directive**: European Union Directive 95/46/EC or any successor to it, together with all other laws about the privacy of

citizens or residents of the member state of the European Economic Area in which you reside or are established as a business enterprise.

14. **Direct Payments API**: Functionality for performing credit and debit card transactions, where the card details are entered online by the cardholder.
15. **Express Checkout**: Functionality for expediting online retail checkout by using information provided to you by PayPal. Details about Express Checkout appear on the **PayPal Website** and in the documentation that PayPal provides for Website Payments Pro.
16. **Hosting Option**: As defined in 1(1) above.
17. **Monthly Fee**: A fee payable on a monthly basis as required in clause 2 above.
18. **Online Card Payment Services**: Functionality provided online by PayPal to enable merchants to receive payments directly from a payer's card (without the funds passing via the payer's PayPal Account), without the card being present at the website or other point of sale. Online Card Payment Services are integral to the Products such as Direct Payments API and Virtual Terminal. PayPal Here™ is not an Online Card Payment Service because the card is present at a physical point of sale.
19. **PayPal Hosted Solution**: PayPal's Direct Payments API integrated into the payment process of your website pursuant to clause 1(1), with that API being operated entirely on PayPal's server (rather than on your website).
20. **PayPal Website**: The website provided by PayPal for the country in which you reside. In the case of the UK, the PayPal Website is currently at http://www.paypal.co.uk. References to PayPal Websites for other countries can be found via a link from any other PayPal Website.
21. **PCI DSS**: Payment Card Industry Data Security Standard, which consists of specifications prescribed by Card Associations to ensure the data security of Card Transactions. A copy of PCI DSS is available online from **https://www.pcisecuritystandards.org/**.
22. **Product**: "Your Product" means whichever one of the Products you access and use after accepting this Agreement.
23. **Qualified Security Assessor** has the meaning given it in PCI DSS.
24. **Recurring Payments Tool**: Technology provided by PayPal for setting up payments that recur at specified intervals or frequencies with authorisation from the payer. See the PayPal Website and product documentation for further information.
25. **Shared Customer**: A person who both has a PayPal Account and is also your customer.
26. **Standard PayPal Payments**: All Payments which you receive from another PayPal account or payments via PayPal's Account Optional Service.

27. **User Agreement**: The contract entered into online as part of the online registration process required to open a PayPal Account. The current User Agreement is to be found via a link from the footer of nearly every page on the PayPal Website. It includes certain policies, notably the Acceptable Use Policy and Privacy Policy, which are also listed on the PayPal Website.
28. **Virtual Terminal**: Functionality provided by PayPal to enable you to receive a card payment by manually entering Card Data given you by the cardholder. Virtual Terminal is one of the Online Card Payment Services
29. **Website Payments Pro**: A suite of functionality consisting of Express Checkout, Direct Payments API, Virtual Terminal and Fraud Management Filters as standard. Optional additional services include Advanced Fraud Management Filters and the Recurring Payments Tool. Website Payments Pro is one of the Online Card Payment Services.

Schedule 1
Data Security Requirements

Website Payment Pro and Virtual Terminal enable you to accept payments online directly from debit and credit cards, which are payment instruments whose security depends on controlling the disclosure of Card Data. A person who has sufficient Card Data can send or receive a card payment charged to the cardholder's account without necessarily having the cardholder's authorisation for the payment. To prevent your Shared Customers from having their Card Data misused, you must keep Card Data secret at all times. Laws transposing the Data Protection Directive also require you to keep a Shared Customer's personal data secure.

PayPal strongly recommends that you obtain the services of a competent professional expert in information security to advise you and assist in securing your website and any other points of sale.

Principles of Data Security

1. **Design and development**. You must design and develop your Critical Systems and all payment-related processes so that they are secure from intrusion and interference by unauthorised persons. All users of your systems must be required to authenticate themselves to your Critical

Systems, and those Systems must limit the access and powers of their users. You must also organise your business so as to segregate critical duties and create controls and checkpoints in your operations, rather than place too much unchecked power over your systems and operations in one person. Never give a user more power over your systems and processes than the minimum necessary for the user to perform his or her assigned role.

2. **Protection against intrusion**. You must divide your operations into two basic categories, (1) those functions available to all users including those outside your organisation, and (2) those available only to trusted people within your organisation. You must employ a firewall to block untrusted users from the using internal-only functions of your Critical Systems. Your web servers and other external-facing portions of your Critical Systems must use well developed and thoroughly tested technology, and make available externally only those functions which are necessary for Shared Customers and other external users to use. Strip your external-facing servers of all superfluous functions to protect (harden) them and reduce their vulnerability to external attack.
3. **Access controls**. Your Critical Systems must restrict access to Card Data and all other personal or important data to only trusted persons within your organisation, and no such person should have greater access to such data than is necessary for that person to perform his or her role. Your systems must track and log all access, use, modification and deletion of Card Data and other personal or important data so that you maintain an audit trail of all such actions. You must also limit access to your Critical Systems and the resources on which they depend such as networks, firewalls, and databases.
4. **Data minimisation**. As a general principle, you should gather and retain no more Card Data or other sensitive data than you need. Holding Card Data and personal data creates a risk of liability to you, and you can reduce that risk by taking and holding less data. If you store Card Data, consider carefully the need to do so: PayPal must refund a payment which lacks its payer's authorisation, and if the user will authorise a further payment, the user will generally also give you up-to-date Card Data again, so you may have little need to store Card Data for future use. Card Data that you do not have is data that you cannot spill if you suffer a Data Breach.
5. **Changes and testing**. Except in emergencies, avoid changing Critical Systems without first planning, testing, and documenting the change, unless the change is routine (*e.g.* adding a user, changing a password, updating inventory and prices). For major systemic changes or those which can impact the security or availability of your Critical Systems, planned changes should be escalated for approval by high-ranking

managers other than the planners of those changes. Implement planned changes in your production systems only after they have been thoroughly tested in a non production environment. Conduct all such testing under the supervision of the your risk management department or others in your company with particular responsibility for its losses.

6. **Audits**. You must audit the operations and security of your Critical Systems at least once a year. This systems audit must be distinct from any audit of your finances. Use trusted and independent experts to audit your Critical Systems, and if you use your employees as auditors, ensure their independence by protecting their employment from retaliation and by isolating them from the work of administering, operating, changing and testing your Critical Systems.
7. **Outsourcing and organisational control**. You must ensure that all persons who have access to your Critical Systems, or who design, develop, operate, maintain, change, test and audit your Critical Systems comply with this Agreement and PCI DSS. You are responsible to ensure compliance even if such persons are not your employees.

What to do in case of a Data Breach

8. **Data Breach**. If you experience a Data Breach, you agree to do all of the following:
    a. Take whatever action you can to stop the Data Breach and mitigate its consequences immediately after discovering the Data Breach.
    b. Notify PayPal as soon as possible after discovering the Data Breach by contacting your account manager (if one is assigned to you) or contacting our Customer Service (details of how to contact us are on the **"Contact Us"** page). If you cannot simultaneously do (a) and notify PayPal, then do (a) first and then notify PayPal.
    c. Notify all Shared Customers whose Card Data has been exposed or which is likely to have been exposed, so that those Shared Customers can take steps to prevent misuse of the Card Data. You further agree to complete this notification immediately after you perform (a) and (b) above, to notify PayPal when you have completed this notification, and to provide a list of Shared Customers whom you have notified. If you fail to complete this step promptly after the Data Breach, PayPal may notify Shared Customers of the Data Breach, and will identify the Shared Customers from your PayPal Account records of who has paid you using a card.
    d. If requested by PayPal, have an independent third party auditor, approved by PayPal, conduct a security audit of your Critical Systems and issue a report. You agree to comply with PayPal's request under this clause at your own expense. You must provide a

copy of the auditor's report to PayPal, and PayPal may provide copies of it to the banks (including, without limitation, Acquiring Institutions) and Card Associations involved in processing card transactions for PayPal. If you do not initiate a security audit with 10 business days of PayPal's request, PayPal may conduct or obtain such an audit at your expense. See also Schedule 1 on Audit.

e. Cooperate with PayPal and follow all reasonable instructions from PayPal to avoid or mitigate consequences of the Data Breach, to improve your Critical Systems so that they satisfy the requirements this Agreement, and to help prevent future Data Breaches. However, PayPal shall not require you to do more than this Agreement requires, unless the additional measures are reasonable in light of the risk to Shared Customers and the best practices of online retailing.
f. Resume normal operation of your Critical Systems only when you have ascertained how the Data Breach occurred and taken all reasonable steps to eliminate the vulnerabilities that made the Data Breach possible or which could make other Data Breaches possible;
g. Report the Data Breach to law enforcement authorities, cooperate in any investigation that they undertake, and cooperate as the authorities may request in order to identify and apprehend the perpetrator of the Data Breach.
h. Refrain from using Card Data that have been exposed or modified in the Data Breach. However, this clause does not prevent you from obtaining and using Card Data again from Shared Customers affected by the Data Breach, after the vulnerabilities in your Critical Systems have been remedied pursuant to (f) above.

Data protection

9. **You as data controller**. You confirm that you are the data controller (as defined in the Data Protection Directive) for all personal data of Shared Customers that you collect and store.

10. **Your compliance with European privacy laws**. You agree to comply with all applicable laws and regulations, including without limitation, the laws of your country that transpose the Data Protection Directive or any successor to it and any rules or guidance by the data protection regulator of your country.

Card Data and PCI DSS

11. **Retention of Card Data**. Unless you receive and record the express consent of the cardholder, you may not retain, track, monitor or store any Card Data. You must completely and securely destroy all Card Data that you retain or hold within 24 hours after you receive an authorisation decision from the issuer relevant to that Card Data.

If, with the cardholder's consent, you briefly retain Card Data, you may do so only to the extent that the Card Data are necessary for processing payment transactions with the cardholder's authorisation. You must never give or disclose the retained Card Data to anyone, not even as part of the sale of your business. Moreover, and regardless of anything to the contrary, you must never retain or disclose the card verification and identification data printed in the signature stripe on the back of the card (i.e. the CVV2 Data), not even with the cardholder's consent.

12. **Card Data that you must not store**. Notwithstanding the immediately preceding clause, you agree to not store any personal identification number (PIN) data, AVS Data, CVV2 Data, or data obtained from the magnetic stripe or other digital storage facility on the card (unless that data is also printed or embossed on the front of the card) of any cardholder. Card associations may impose fines if you violate this clause, which reflects card association rules. In this clause, 'store' means retain in any form, whether digital, electronic, paper-based, or otherwise, but does not include temporary capture and holding of data while it is actively being processed (but not afterwards).

13. **Merchant's use of Card Data**. You agree not to use or disclose Card Data except for the purposes of obtaining authorisation from the card issuer, completing and settling the Card Transaction for which the Card Data was given to you, together with resolving any Chargeback or Reversal Dispute, or similar issues involving Card Transactions. PayPal is required by banking laws to refund payments lacking the payer's authorisation, so your use of Card Data to carry out a Card Transaction must be authorised by the cardholder or it will subject to Reversal.

14. **Secure storage and disposal of Card Data**. You agree to:
    a. establish and maintain sufficient controls for limiting access to all records containing Card Data;
    b. not sell or disclose to a third party any Card Data or any information obtained in connection with a Card Transaction;

c. keep no Card Data on paper or in portable digital storage devices such as USB memory devices or removable disks;
d. not reproduce any electronically captured signature of a cardholder except on PayPal's specific request; and
e. destroy Card Data either by destroying the medium on which the Card Data are stored or by erasing or rendering the Card Data completely and irreversibly unintelligible and meaningless.

If you transfer your business, Card Data and any information you have about Card Transactions is not transferable under Card Association rules as an asset of the business. In such cases, you agree to provide the Card Data and any transactional data to PayPal if it requests. If PayPal does not request such data, you must destroy it when your business transfers.

15. **PCI DSS audit**. If PayPal so requests, you agree that a Qualified Security Assessor may conduct a security audit of your systems, controls and facilities and issue a report to PayPal and the Associations. You agree to cooperate fully in the conduct of this audit, and to provide any information and access to your systems required by the auditor for the performance of the audit. You also agree to bear the reasonable expenses of this audit. If you fail to initiate such an audit after PayPal requests you to do so, you authorise PayPal to take such action at the Merchant's expense, or PayPal may immediately suspend your use of your Product. You will receive a copy of the audit report, and PayPal must also receive a copy and provide a copy to any Acquiring Institution or Card Association that requests a copy.

Updated PayPal Website Payments Pro and Virtual Terminal Agreement

This version of the Agreement will take effect on January 9, 2018. Changed text is shown underlined.

This PayPal Website Payments Pro / Virtual Terminal Agreement ("Agreement") is a contract between you (also referred to as the “Merchant”) and PayPal (Europe) S.àr.l. et Cie, S.C.A. ("PayPal" or "we"). You agree that any use by you of Online Card Payment Services shall constitute your acceptance of this Agreement and we recommend that you store or print-off a copy of this Agreement. PayPal is licensed as a Luxembourg credit institution and is under the prudential supervision of the Luxembourg supervisory authority, the Commission de Surveillance du Secteur Financier (the "CSSF"). The CSSF has its registered office in L-1150 Luxembourg. Because the funds in your PayPal Account are electronic money, which does not legally qualify as a deposit or an investment service, you are not protected by the Luxembourg deposit guarantee schemes provided by the Association pour la Garantie des Dépôts Luxembourg.

This Agreement applies to your use of PayPal Website Payments Pro and/or Virtual Terminal (the "Products"). To proceed with obtaining one or both of the Products, you must read, agree with and accept all of the terms and conditions contained in this Agreement.

We may make Changes to this Agreement by giving notice of such Change by posting a revised version of this Agreement on the PayPal website(s). A Change will be made unilaterally by us and you will be deemed to have accepted the Change after you have received notice of it. We will give you 2 months' notice of any Change with the Change taking effect once the 2 month notice period has passed, except the 2 month notice period will not apply where a Change relates to the addition of a new service, extra functionality to the existing Service or any other change which neither reduces your rights nor increases your responsibilities. In such instances, the change will be made without notice to you and shall be effective immediately upon giving notice of it. All future Changes set out in the **Policy Update** already published on the “Legal Agreements” landing page of the PayPal website at the time you register for the Online Card Payment Services are incorporated by reference into this Agreement and will take effect as specified in that **Policy Update**.

If you do not accept any Change, you must close your Account following the account closure procedure set out in the User Agreement. If you do not object to a Change by closing your Account within the 2 month notice period, you will be

deemed to have accepted the Change. While you may close your Account at any time and without charge, please note that you may still be liable to us after you terminate this Agreement for any liabilities you may have incurred and are responsible for prior to terminating this Agreement and please further note our rights under the User Agreement.

Capitalised terms are defined below. Please view **download and save** this agreement.

1. Setting up and activating your Product

1. **Getting started.** To obtain and use your Product, you must first do all of the following:
    a. Complete the online application and approval process for your Product, open a PayPal Business Account (if you do not already have one), and follow the instructions set out in PayPal's online process to access and use your Product.
    b. Integrate your Product into the payment process of your website, if your Product is Website Payments Pro. You are not required to integrate your Product into the payment process of your website if you only access and use Virtual Terminal. PayPal is not responsible for any problems that could occur by integrating your Product into your 'live' website.
    c. Activate your Product by using it in a 'live' payment transaction for the first time.

    If your Product is Website Payments Pro, you may only integrate and use Website Payments Pro in one of the following mutually exclusive ways - either (i) as a PayPal Hosted Solution (in which PayPal operates Website Payments Pro for you as a PayPal-hosted service) or (ii) operated on your own facilities - (each option being a **"Hosting Option")**. PayPal may (but, notwithstanding any other provision in this Agreement, shall not be obliged to) provide both Hosting Options. PayPal may, at its sole discretion, set either Hosting Option as your default option for integrating the Direct Payments API into the payment process of your website.

2. **Required use of Express Checkout.** If your Product is Website Payments Pro, you must implement PayPal Express Checkout as part of

your website integration; see clause 2(1) below. In implementing Express Checkout, you agree that your website:

a. Includes a PayPal Express Checkout button either: (A) before you request the shipping/billing address and other financial information from your customers or (B) on the same page that you collect such information if you only use one page for your checkout process.
b. Offers PayPal as a payment option together with the other payment options you offer for Express Checkout. The PayPal logo must be displayed with equal or greater prominence as the logos for your other payment options.
c. Provides your customers with the option of not storing their personal information, including their email address, shipping/billing address, and financial information, as part of the checkout process.

Failure to implement Express Checkout affects the fees you pay; see clause 2(1) and 2(3).

3. **Your information.** You confirm that you have read, consented and agreed to PayPal's Privacy Policy, which explains the information that we collect about you and your online business. In particular, you agree and consent that PayPal may obtain from a third party your credit history and financial information about your ability to perform your obligations under this Agreement; the PayPal Privacy Policy lists the companies involved in this exchange of credit-related information. PayPal will review your credit and other risk factors of your Account (reversals and chargebacks, customer complaints, claims etc.) on an ongoing basis, and we may also review your website and the products for sale on it. PayPal will store, use and disclose all information that we have about you in conformity with PayPal's Privacy Policy.

5. **Cancellation.** PayPal may terminate your access to and/or use of either or both Products and / or terminate this Agreement at any time before the Activation Date by notifying you.

2. Fees

1. **How fees are paid**. You agree to pay the fees in this Agreement as they become due without set-off or deduction. You authorise PayPal to (and PayPal may) collect Monthly Fees first from any available Balance in your Account and then also from the funding source(s) registered for your Account, and you authorise PayPal to (and PayPal may) collect fees for receiving payments from the payments you receive before those funds are

credited to your account. If PayPal is unable to collect a past due fee from your Account and its funding source(s), we may take action against you as provided in the User Agreement for unpaid fees.

Except as further provided in this Agreement, you agree to pay the fees set out in the User Agreement.

Fees will be charged in the currency of the payment received.

See the Glossary at clause 2.6 for further reference.

2. **Monthly Fees**

Product	**Monthly Fee**
Website Payments Pro (including Express Checkout, Direct Payments API, Virtual Terminal and Fraud Management Filters)	GBP 20.00
Virtual Terminal only	GBP 20.00

3.

3. **Transaction Fees for Standard PayPal Payments with Express Checkout**

If you receive the payment:	**the PayPal Standard Rate fee is:**	**the PayPal Merchant Rate is as follows:**	
		where the aggregate monetary amount of payments received in your PayPal Account in the previous calendar month is:	**the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:**
as a Standard PayPal Payment using Express Checkout	3.4% + Fixed Fee	GBP 0.00 - GBP 1,500.00	3.4% + Fixed Fee
		GBP 1,500.01 - GBP 6,000.00	2.9% + Fixed Fee

		GBP 6,000.01 - GBP 15,000.00	2.4% + Fixed Fee
		GBP 15,000.01 – GBP 55,000.00	1.9 % + Fixed Fee
		Above GBP 55,000.00	1.4 % + Fixed Fee

4.

4. **Transaction Fees for Card Payments under the Blended Pricing Fee Structure**

If you receive a payment:	**the PayPal Standard Rate fee is:**	**the PayPal Merchant Rate is as follows:**	
		where the aggregate monetary amount of payments received in your PayPal Account in the previous calendar month is:	**the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:**
from a card (Visa, MasterCard or Maestro) using the Online Card Payment Services	3.4% + Fixed Fee	GBP 0.00 - GBP 1,500.00	3.4% + Fixed Fee
		GBP 1,500.01 - GBP 6,000.00	2.9% + Fixed Fee
		GBP 6,000.01 - GBP 15,000.00	2.4% + Fixed Fee
		Above GBP 15,000.00	1.9 % + Fixed Fee

5.

5. **Transaction Fees for Card Payments under the Interchange Plus Fee Structure**

If you receive a payment:	the PayPal Standard Rate fee is:	the PayPal Merchant Rate is as follows:	
		where the aggregate monetary amount of payments received in your Account in the previous calendar month is:	the PayPal Merchant Rate fee (subject to the further terms and conditions in this section 2.8) is:
from a card (Visa, MasterCard or Maestro) using the Online Card Payment Services	Interchange Fee (approximately ranges from 0.2% to 2.0%) + 2.9% + Fixed Fee	GBP 0.00 - GBP 1,500.00	Interchange Fee + 2.9% + Fixed Fee
		GBP 1,500.01 - GBP 6,000.00	Interchange Fee + 2.4% + Fixed Fee
		GBP 6,000.01 - GBP 15,000.00	Interchange Fee + 1.9% + Fixed Fee
		Above GBP 15,000.00	Interchange Fee + 1.4% + Fixed Fee

6.

6. **Glossary**

a. Interchange Fees are set by Visa and MasterCard. They approximately range from 0.2% to 2.0% and vary for different types of cards (for example by categories and brand). **PayPal shall always charge you the Interchange Fee as set by Visa and MasterCard and as passed on by its Acquirer.** Single Interchange Fees may change from time to time. For more information on Interchange Fees, please see **MasterCard's** and **Visa's**website as well as our **simplified overview**.

b. Percentage-based fees (such as 3.4%) refer to an amount equal to that percentage of the payment amount.

c. Fixed Fees are based on the currency received, as follows:

Argentine Peso:	2.00 ARS	New Zealand Dollar:	$0.45 NZD
Australian Dollar:	$0.30 AUD	Norwegian Krone:	2.80 NOK
Brazilian Real:	0.60 BRL	Philippine Peso:	15.00 PHP
Canadian Dollar:	$0.30 CAD	Polish Zloty:	1.35 PLN
Czech Koruna:	10.00 CZK	Russian Ruble	10.00 RUB
Euro:	€0.35 EUR	Singapore Dollar:	0.50 SGD
Danish Kroner:	2.60 DKK	Swedish Kronor:	3.25 SEK
Hong Kong Dollar:	$2.35 HKD	Swiss Franc:	0.55 CHF
Hungarian Forint:	90 HUF	Taiwan New Dollar:	10.00 TWD
Israeli New Shekels:	1.20 ILS	Thai Baht:	11.00 THB
Japanese Yen:	¥40 JPY	Turkish Lira:	0.45 TRY
Malaysian Ringgit:	2 MYR	**UK Pounds Sterling:**	**£0.20 GBP**
Mexican Peso:	4.00 MXN	US Dollar:	$0.30 USD

7.

7. **Blended Pricing or Interchange Plus Transaction Fees?**

When you receive card payments using any of our Online Card Payment Services (including via Direct Payment API or Virtual Terminal):

a. The Blended Pricing fee structure shall apply until 23 June 2016 ("**Interchange Plus Launch**").
b. You may choose the fee structure applicable to you on or after Interchange Plus Launch, by the methods or procedures that PayPal may make available to you before and after Interchange Plus Launch. If you do not make an election, you will stay on your existing fee structure.
c. You may choose your fee structure for future transactions only, not for past transactions. The fee structure that applies when you receive card payments using any of our Online Card Payment Services also applies when you receive card payments using PayPal Here™. This means that if you opt to be charged under the Interchange Plus fee structure, the respective Interchange Plus fee structure will apply to the use of both our Online Card Payment Services and PayPal Here.

8. **Merchant Rate**

   Merchant Rate applies only to Accounts with Merchant Rate status. Merchant Rate status is subject to eligibility, application and approval by PayPal. PayPal may evaluate applications on a case-by-case basis, including, without limitation, on the following criteria: qualifying monthly sales volume, size of average shopping cart and an Account in good standing. To be eligible to apply for (and retain) PayPal Merchant Rate status the Account must:

   - at all times be in good standing and not under investigation; and
   - have received more than £1,500.00 GBP in aggregate monetary amount of payments in the previous calendar month.

   PayPal may downgrade an Account to the Standard Rate at any time if the above conditions are not met or there are unresolved chargebacks against the Account or as otherwise provided for under the provisions relating to the Merchant Rate in the User Agreement.

   If PayPal downgrades your Account you will need to apply to PayPal again for your Account to get Merchant Rate status.

   You may apply to receive Merchant Rate for your Account using the dedicated online **application form** when logged into your PayPal Account. If your application is rejected, please note that you may only submit an application once every thirty days.

9. **Additional Transaction Fees**

   a. Receiving Cross Border Payments

   The fee for Receiving Cross Border payments applies as outlined in the User Agreement, except that it does not apply to payments received from **cards using the Online Card Payment Services under the Interchange Plus fee structure**.

   b. Failure to implement Express Checkout. If you do not implement Express Checkout as required in clause 1 (2) above, the percentage components of the Transaction Fees set out in clause 2.2 will each increase by an additional 0.5 % after PayPal gives you 30 days' notice. You agree to pay the increased fees.

c. Additional risk factors. If PayPal determines that your Account receives, or is likely to receive, a disproportionately high number of customer complaints, Reversals, Chargebacks, Claims, or other indicators of a serious level of risk, PayPal may increase the percentage components of your Transaction Fees by up to 5%, after giving you 30 days prior notice of the increase. You agree to terminate your use of the Product if you do not agree to this increase.

10. **Other Fees**

Activity/Event/Product	Fee
. **Recurring Payment Tool (optional service)**	GBP 20.00 per month
b. **Uncaptured Authorisation Transactions**	GBP 0.20 for each successful but uncaptured authorisation transaction via Direct Payment API or Virtual Terminal
c. **Card Account Verification Transactions**	0.20 GBP for each card account verification request (for all Direct Payment API or Virtual Terminal card account verification transactions (Visa and MasterCard only). For the avoidance of doubt, this does not include Uncaptured Authorisation Transactions.

11. **MasterCard transactions**. For further information about MasterCard's rules and rates, please visit: **http://www.mastercard.com/us/merchant/index.html**.

12. **Monthly Reports on Transaction Costs**. PayPal shall make available monthly reports on transaction costs (inclusive of interchange fees) for card transactions which you process with PayPal Website Payments Pro and Virtual Terminal. These reports will be downloadable from your PayPal Account. The reports do not include any Standard PayPal payments.

3. Settlement of Card Payments within the Interchange Plus Fee Structure

You agree that, when PayPal receives a card payment for you, PayPal may hold those funds in your Reserve Account and you are thereby giving a Payment Order that instructs PayPal to pay those funds to your Payment Account only on the Business Day on which PayPal receives the information about the interchange fee applicable to the card payment, at which time the funds will then be made available to you in your Payment Account. While the funds are held in your Reserve Account, the transaction will appear to you as "Pending" in your Account details. PayPal does not consider that the proceeds of the card payment in your Reserve Account are at your disposal until PayPal has received the information on the applicable interchange fee from our Processor (which can be within the next Business Day following the day on which the card payment was initiated by the card holder).

4. Information security

1. **Compliance with Data Security Schedule**. You agree (as a "Merchant") to comply with Schedule 1 below, which forms part of this Agreement.
2. **Your PCI DSS compliance**. You also agree to comply with the PCI Data Security Standard (PCI DSS). You must protect all Card Data that comes within your control according to PCI DSS, and you must design, maintain and operate your website and other systems in conformity with PCI DSS. You must ensure that your staff are and remain sufficiently trained so that they are aware of PCI DSS and can carry out its requirements. PayPal is not responsible for any costs that you incur in complying with PCI DSS.
3. **PayPal's PCI DSS compliance**. PayPal warrants that PayPal and your Product comply and will comply with PCI DSS. However, PayPal's compliance, and your Product's, are not sufficient to achieve compliance with PCI DSS by you and your systems and processes.
4. **3D Secure**. Requirements of the European Central Bank and PayPal's bank regulators require use of 3D Secure in certain circumstances, and Card Associations may also require it to reduce an excessive number of Card Transactions unauthorised by the cardholder. PayPal may by notice to you require that you implement 3D Secure for all or certain specified Card Transactions. You agree to implement 3D Secure if required in such

a notice, where the issuer of a particular card supports 3D Secure for that card.

5. **Price and currency**. You may not submit payment transactions in which the amount is the result of dynamic currency conversion. This means that you may not list an item in one currency and then accept payment in a different currency. If you are accepting payments in more than one currency, you must separately list the price for each currency.

5. User Agreement

1. **User Agreement applies**. You acknowledge and agree that the User Agreement, and not this Agreement, is the "framework contract" between you and PayPal as defined in laws transposing the Second Payment Services Directive ((EU)2015/2366). The terms of the User Agreement also apply to you and are incorporated by reference into this Agreement. The definition of "Services" in the User Agreement shall be amended to include your Product, and the definition of "Agreement" shall include this Agreement. In case of any inconsistency between this Agreement and the User Agreement, this Agreement supersedes the User Agreement, but only to the extent of that inconsistency. Where this Agreement and the User Agreement both specify a fee for the same action, the fee specified in this Agreement will apply rather than the fee in the User Agreement. The User Agreement can be found via a link in the footer of nearly every PayPal web page. The User Agreement includes important provisions which:
    a. Permit PayPal to take a Reserve to secure your obligation to pay Chargebacks, Reversals and fees;
    b. Obligate you to follow PayPal's Acceptable Use Policy in your use of PayPal;
    c. Give legal effect to PayPal's Privacy Policy, which governs our use and disclosure of your information and that of Shared Customers; and
    d. Permit PayPal to restrict a payment or your PayPal Account in circumstances listed in the User Agreement.
2. **Failed payments and Product tools**. You are responsible for Chargebacks, Reversals and other invalidated payments as provided in the User Agreement, regardless of how you use and configure your Product, including its fraud filtering technology and similar preventive tools (if any). Those tools can be useful in detecting fraud and avoiding payment failures, but they do not affect your responsibility and liability pursuant to the User Agreement for Chargebacks, Reversals and payments which are otherwise invalidated.

6. Intellectual property and ID codes

1. **Licence**. PayPal hereby grants to you a non-exclusive, non-transferable, revocable, non-sublicenseable, limited license to (a) use your Product in accordance with the documentation provided on the PayPal Website; and to (b) use the documentation provided by PayPal for your Product and reproduce it for internal use only within your business. Your Product as licensed is subject to change and will evolve along with the rest of the PayPal system; see clause 8(1). You must comply with the implementation and use requirements contained in all PayPal documentation and instructions accompanying the Product issued by PayPal from time to time (including, without limitation, any implementation and use requirements we impose on you to comply with applicable laws and card scheme rules and regulations).
2. **ID codes**. PayPal will provide you with certain identifying codes specific to you. The codes identify you and authenticate your messages and instructions to us, including operational instructions to PayPal software interfaces. Use of the codes may be necessary for the PayPal system to process instructions from you (or your website). You must keep the codes safe and protect them from disclosure to parties whom you have not authorised to act on your behalf in dealing with PayPal. You agree to follow reasonable safeguards advised by PayPal from time to time in order to protect the security of those identifying codes. If you fail to protect the security of the codes as advised, you must notify PayPal as soon as possible, so that PayPal can cancel and re-issue the codes. PayPal may also cancel and re-issue the codes if it has reason to believe that their security has been compromised, and after notifying you whenever notice can reasonably be given.
3. **Ownership of PayPal Website Payments Pro information and materials**. As part of Merchant's access to, and utilisation of PayPal Website Payments Pro, Merchant will be provided with certain information and materials (the "Pro Materials") which are able to be used by Merchant to use PayPal Website Payments Pro. All intellectual property rights associated with the Pro Materials remain the property of PayPal or the relevant Acquiring Institution(as the case may be). Merchant agrees to not give, transfer, assign, novate, sell, resell (either partly or in whole) the Pro Materials to any person.

7. Banking terms for Card Transactions

1. PayPal utilises services from banking partners in processing Card Transactions, including both direct payments to you from a card as well as Card Transactions that fund a PayPal payment to you. The **Commercial Entity Agreements** apply in relation to those services. In accepting this Agreement, you also accept the **Commercial Entity Agreements**, which form part of this Agreement. A copy of the Commercial Entity Agreements can be obtained from the Legal link at the bottom of a PayPal web page.

8. Termination and suspension

1. **By you**. You may terminate this Agreement by doing either of the following:
    a. Giving 10 days' notice to PayPal Customer Service on of your intent to terminate this Agreement. PayPal Customer Service will confirm termination via email. This option lets you stop using your Product and paying for it, but your PayPal Account remains open and its User Agreement remains in effect.
    b. Closing the PayPal Account that you use with your Product (see the User Agreement for more information).
2. **By PayPal**. PayPal may terminate this Agreement by doing any of the following:
    a. Giving you 2 months' notice by email to you at your registered email address associated with your Account of PayPal's intent to terminate this Agreement. Unless otherwise notified, terminating this Agreement does not affect your User Agreement and your PayPal Account remains open.
    b. Terminating the User Agreement that applies to the PayPal Account used with your Product.
3. **By events**. PayPal may terminate this Agreement immediately without notice if you:
    a. Breach this Agreement or the User Agreement;
    b. Become unable to pay or perform your obligations as they fall due;
    c. Become unable to pay your debts (within the meaning of section 123 of the Insolvency Act 1986), admit your inability to pay your debts or otherwise become insolvent;
    d. Have any distraint, execution, attachment or similar action taken, levied or enforced against you or your assets, or if any garnishee order is issued or served on you;
    e. Become the subject of any petition presented, order made or resolution passed for the liquidation, administration, bankruptcy or dissolution of all or a substantial part of your business, except where

solvent amalgamation or reorganisation is proposed on terms previously approved by PayPal,

f. Lose full and unrestricted control over all or part of your assets because of the appointment of a receiver, manager, trustee, liquidator or similar officer;
g. Enter into or proposes any composition or arrangement concerning your debts with your creditors (or any class of its creditors);
h. A material adverse change occurs in your business, operations, or financial condition; or
i. You provide inaccurate information in applying for your Product or in your dealings with us.

4. **Effect of termination**. When this Agreement terminates, you must immediately stop using your Product, and PayPal may prevent or hinder you from using it after termination. If you nevertheless use a Product after termination of this Agreement, then this Agreement will continue to apply to your use of that Product until you give effect to the termination by stopping your use of that Product. The following clauses in this Agreement shall survive termination of this agreement and continue in full force and effect: Clauses 2, 4(1) 8(2), 8(4). Termination of this agreement shall not affect any rights, remedies or obligations of the parties that have accrued or become due prior to termination, and you will not be entitled to a refund of any Monthly Fee paid prior to termination.
5. **Breach and suspension**. If you breach this Agreement, the User Agreement, or a security requirement imposed by PCI DSS, PayPal may immediately suspend your use of your Product (in other words, we may render your Product temporarily inoperable). PayPal may require you to take specified corrective actions to cure the breach and have the suspension lifted, although nothing in this Agreement precludes PayPal from pursuing any other remedies it may have for breach. In addition, if PayPal reasonably suspects that you may be in breach of this Agreement or PCI DSS, PayPal may suspend your use of your Product pending further investigation.

   If PayPal suspends your access to or use of PayPal Website Payments Pro, PayPal will notify you and explain the basis of PayPal's actions in suspending your use of your Product, and may specify corrective actions to cure the breach and have the suspension lifted. PayPal's suspension of the Merchant's access or use of PayPal Website Payments Pro will remain in effect and until such time as PayPal is satisfied that the Merchant has remedied the applicable breach(es).

9. Miscellaneous

1. **Future of the Products**. PayPal retains sole and absolute discretion in determining (a) the future course and development of the Products, (b) which improvements to make in them and when, and (c) whether and when defects are to be corrected and new features introduced. PayPal welcomes feedback from users in planning the future of the Products but is not required to act in accordance with any feedback received. In giving us feedback, you agree to claim no intellectual property interest in your feedback.
2. **No warranty**. Your Product and all accompanying documentation are provided to you on an "as is" basis. PayPal does not give or offer any warranty, express or implied, by operation of law or otherwise, in relation to your Product, the licensed software or user documentation provided. Nothing provided by PayPal under this Agreement or otherwise for your Product has PayPal's authorisation to include a warranty, and no obligation or liability will arise out of PayPal's rendering of technical, programming or other advice or service in connection with any Product, licensed software and user document provided (including, without limitation, services that may assist you with the customisation of your Product). PayPal recommends that you test the implementation of your Product thoroughly as PayPal is not responsible for any loss caused by a defect in it.

   If PayPal hosts your Product (in other words, we run the software for you as a web service), PayPal does not guarantee continuous, uninterrupted or secure access to your hosted Product. PayPal will not be liable for any delay or failure in hosting your Product. You acknowledge the availability of your Product for use may be occasionally limited to allow for repairs, maintenance or the introduction of new facilities or services.

3. **Indemnity**. You agree to indemnify PayPal and keep PayPal fully indemnified on a continuing basis from any direct loss, damage and liability, and from any claim, demand or cost (including reasonable attorneys' fees) incurred in relation to any third party (including a Shared Customer) and arising out of your breach of this Agreement, the User Agreement and the documents incorporated in it by reference (including the Acceptable Use Policy), or the violation of any law.

4. **PayPal Hosted Solution and your intellectual property**. You hereby grant to PayPal a royalty-free, worldwide non-exclusive licence to use your or any of your affiliates' names, images, logos, trademarks, service marks, and/or trade names as you may provide to PayPal when using the Products ("Your Marks") for the sole purpose of enabling your use of the Products (including, without limitation, the customisation of your hosted

Product). Title to and ownership of Your Marks and all goodwill arising from any use hereunder will remain with you. You represent and warrant that you have the authority to grant PayPal the right to use Your Marks and you shall indemnify PayPal and keep PayPal fully indemnified on a continuing basis from any claims or losses suffered by it arising from the use of Your Marks in connection with the Products.

5. **Assignment, amendment and waiver**. You may not assign this Agreement without first obtaining PayPal's written consent. PayPal may assign, novate or otherwise transfer this agreement without your consent by notifying you. Neither party may amend this Agreement or waive any rights under it except in a written document signed by both parties.

6. **English law and jurisdiction**. This Agreement is governed by English law. The parties submit to the non-exclusive jurisdiction of the courts of England and Wales.

10. Definitions

Capitalised terms not listed in this clause are defined in the User Agreement.

1. **3D Secure**: A security procedure that enables a card-issuing bank to authenticate the cardholder authorising a Card Transaction at the time a payment is made. 3D Secure has other brand names depending on the Card Association whose branding appears on the card; brand names for 3D Secure include Verified by Visa and MasterCard SecureCode.
2. **Account Nationality**: The "Account Nationality" of a PayPal Account is the same as that of the bank account into which PayPal E-money is withdrawn (redeemed). For example, if a Spanish bank account is registered as the account into which PayPal E-money is withdrawn, then the Account Nationality of the PayPal Account from which that redemption occurs is Spanish. A PayPal Account from which E-money is withdrawn into a German bank account would be German, even though a German and Spanish Account would both be denominated in the same currency (Euros).
3. **Acquiring Institution:** means a financial institution or bank that provides services to you and PayPal to enable you to (a) accept payment by cardholders using cards: and (b) receive value in respect of Card Transactions.
4. **Activation Date**: The date on which you complete all of the steps for "Getting started" as listed in clause 1(1) above.

5. **Advanced Fraud Management Filters** : Technology provided by PayPal to enable you to (a) check a card payment against criteria such as the cardholder's billing address (Address Verification Service or AVS), the card's CVV2 Data, and databases of suspicious addresses, identifiers, and patterns. See the PayPal Website and product documentation for further information. Advanced Fraud Management Filters offer a greater level of transaction screening, and transactions can be automatically flagged, reviewed or declined based on how you configure the filters.
6. **AVS Data**: Information returned by the Address Verification System operated by or on behalf of Card Associations, which compares address data provided by an apparent cardholder with address data on file for the card at the card issuer.
7. **Card Association**: A company or consortium of financial institutions which promulgates rules to govern Card Transactions that involve the card that carries the company's or the consortium's brand. Examples include Visa USA, Visa Europe, and the other Visa regions; Mastercard International Incorporated; American Express Company and similar organisations.
8. **Card Data**: All personal or financial information relevant to a Card Transaction, including information recorded on the card itself (whether in human-readable form or digitally), together with the cardholder's name and address and any other information necessary for processing a Card Transaction.
9. **Card Transaction**: A payment made using a credit or debit card, an American Express card, or any other payment method using a physical data-carrying item intended to be held in the payer's possession. The Products support only certain types of Card Transactions; see the PayPal Website for more information.
10. **Critical Systems**: The information technology (both hardware and software) that you employ to operate your Products, to protect them and your online points of sale against intrusion and interference, and to store payment-related and personal data, including any Card Data that you retain and all personal data about Shared Customers.
11. **CVV2 Data**: The three-digit number printed to the right of the card number in the signature panel area on the back of the card. (For American Express cards, the code is a four-digit unembossed number printed above the card number on the front of the American Express card.) The CVV2 Data are uniquely associated with each individual plastic card and ties the card account number to the plastic.
12. **Data Breach**: An intrusion into or malfunction of a computer system in which Card Data are stored, and which intrusion or malfunction either (a) exposes, modifies or destroys all or part of the Card Data in the system, or (b) runs a significant risk, in the opinion of a qualified expert in information security, of exposing, modifying or destroying all or part of the Card Data in

the system. Card Data are exposed where they are released from the normal access controls of the system without authorisation, or where they are actually disclosed to one or more unauthorised persons.

13. **Data Protection Directive**: European Union Directive 95/46/EC or any successor to it, together with all other laws about the privacy of citizens or residents of the member state of the European Economic Area in which you reside or are established as a business enterprise.
14. **Direct Payments API**: Functionality for performing credit and debit card transactions, where the card details are entered online by the cardholder.
15. **Express Checkout**: Functionality for expediting online retail checkout by using information provided to you by PayPal. Details about Express Checkout appear on the **PayPal Website** and in the documentation that PayPal provides for Website Payments Pro.
16. **Hosting Option**: As defined in 1(1) above.
17. **Monthly Fee**: A fee payable on a monthly basis as required in clause 2 above.
18. **Online Card Payment Services**: Functionality provided online by PayPal to enable merchants to receive payments directly from a payer's card (without the funds passing via the payer's PayPal Account), without the card being present at the website or other point of sale. Online Card Payment Services are integral to the Products such as Direct Payments API and Virtual Terminal. PayPal Here™ is not an Online Card Payment Service because the card is present at a physical point of sale.
19. **PayPal Hosted Solution**: PayPal's Direct Payments API integrated into the payment process of your website pursuant to clause 1(1), with that API being operated entirely on PayPal's server (rather than on your website).
20. **PayPal Website**: The website provided by PayPal for the country in which you reside. In the case of the UK, the PayPal Website is currently at http://www.paypal.co.uk. References to PayPal Websites for other countries can be found via a link from any other PayPal Website.
21. **PCI DSS**: Payment Card Industry Data Security Standard, which consists of specifications prescribed by Card Associations to ensure the data security of Card Transactions. A copy of PCI DSS is available online from **https://www.pcisecuritystandards.org/**.
22. **Product**: "Your Product" means whichever one of the Products you access and use after accepting this Agreement.
23. **Qualified Security Assessor** has the meaning given it in PCI DSS.
24. **Recurring Payments Tool**: Technology provided by PayPal for setting up payments that recur at specified intervals or frequencies with authorisation from the payer. See the PayPal Website and product documentation for further information.

25. **Shared Customer**: A person who both has a PayPal Account and is also your customer.
26. **Standard PayPal Payments**: All Payments which you receive from another PayPal account or payments via PayPal's Account Optional Service.
27. **User Agreement**: The contract entered into online as part of the online registration process required to open a PayPal Account. The current User Agreement is to be found via a link from the footer of nearly every page on the PayPal Website. It includes certain policies, notably the Acceptable Use Policy and Privacy Policy, which are also listed on the PayPal Website.
28. **Virtual Terminal**: Functionality provided by PayPal to enable you to receive a card payment by manually entering Card Data given you by the cardholder. Virtual Terminal is one of the Online Card Payment Services
29. **Website Payments Pro**: A suite of functionality consisting of Express Checkout, Direct Payments API, Virtual Terminal and Fraud Management Filters as standard. Optional additional services include Advanced Fraud Management Filters and the Recurring Payments Tool. Website Payments Pro is one of the Online Card Payment Services.

Schedule 1
Data Security Requirements

Website Payment Pro and Virtual Terminal enable you to accept payments online directly from debit and credit cards, which are payment instruments whose security depends on controlling the disclosure of Card Data. A person who has sufficient Card Data can send or receive a card payment charged to the cardholder's account without necessarily having the cardholder's authorisation for the payment. To prevent your Shared Customers from having their Card Data misused, you must keep Card Data secret at all times. Laws transposing the Data Protection Directive also require you to keep a Shared Customer's personal data secure.

PayPal strongly recommends that you obtain the services of a competent professional expert in information security to advise you and assist in securing your website and any other points of sale.

Principles of Data Security

1. **Design and development**. You must design and develop your Critical Systems and all payment-related processes so that they are secure from intrusion and interference by unauthorised persons. All users of your systems must be required to authenticate themselves to your Critical Systems, and those Systems must limit the access and powers of their users. You must also organise your business so as to segregate critical duties and create controls and checkpoints in your operations, rather than place too much unchecked power over your systems and operations in one person. Never give a user more power over your systems and processes than the minimum necessary for the user to perform his or her assigned role.
2. **Protection against intrusion**. You must divide your operations into two basic categories, (1) those functions available to all users including those outside your organisation, and (2) those available only to trusted people within your organisation. You must employ a firewall to block untrusted users from the using internal-only functions of your Critical Systems. Your web servers and other external-facing portions of your Critical Systems must use well developed and thoroughly tested technology, and make available externally only those functions which are necessary for Shared Customers and other external users to use. Strip your external-facing servers of all superfluous functions to protect (harden) them and reduce their vulnerability to external attack.
3. **Access controls**. Your Critical Systems must restrict access to Card Data and all other personal or important data to only trusted persons within your organisation, and no such person should have greater access to such data than is necessary for that person to perform his or her role. Your systems must track and log all access, use, modification and deletion of Card Data and other personal or important data so that you maintain an audit trail of all such actions. You must also limit access to your Critical Systems and the resources on which they depend such as networks, firewalls, and databases.
4. **Data minimisation**. As a general principle, you should gather and retain no more Card Data or other sensitive data than you need. Holding Card Data and personal data creates a risk of liability to you, and you can reduce that risk by taking and holding less data. If you store Card Data, consider carefully the need to do so: PayPal must refund a payment which lacks its payer's authorisation, and if the user will authorise a further payment, the user will generally also give you up-to-date Card Data again, so you may have little need to store Card Data for future use. Card Data that you do not have is data that you cannot spill if you suffer a Data Breach.
5. **Changes and testing**. Except in emergencies, avoid changing Critical Systems without first planning, testing, and documenting the change,

unless the change is routine (*e.g.* adding a user, changing a password, updating inventory and prices). For major systemic changes or those which can impact the security or availability of your Critical Systems, planned changes should be escalated for approval by high-ranking managers other than the planners of those changes. Implement planned changes in your production systems only after they have been thoroughly tested in a non production environment. Conduct all such testing under the supervision of the your risk management department or others in your company with particular responsibility for its losses.

6. **Audits**. You must audit the operations and security of your Critical Systems at least once a year. This systems audit must be distinct from any audit of your finances. Use trusted and independent experts to audit your Critical Systems, and if you use your employees as auditors, ensure their independence by protecting their employment from retaliation and by isolating them from the work of administering, operating, changing and testing your Critical Systems.
7. **Outsourcing and organisational control**. You must ensure that all persons who have access to your Critical Systems, or who design, develop, operate, maintain, change, test and audit your Critical Systems comply with this Agreement and PCI DSS. You are responsible to ensure compliance even if such persons are not your employees.

What to do in case of a Data Breach

8. **Data Breach**. If you experience a Data Breach, you agree to do all of the following:
    a. Take whatever action you can to stop the Data Breach and mitigate its consequences immediately after discovering the Data Breach.
    b. Notify PayPal as soon as possible after discovering the Data Breach by contacting your account manager (if one is assigned to you) or contacting our Customer Service (details of how to contact us are on the **"Contact Us"** page). If you cannot simultaneously do (a) and notify PayPal, then do (a) first and then notify PayPal.
    c. Notify all Shared Customers whose Card Data has been exposed or which is likely to have been exposed, so that those Shared Customers can take steps to prevent misuse of the Card Data. You further agree to complete this notification immediately after you perform (a) and (b) above, to notify PayPal when you have completed this notification, and to provide a list of Shared Customers whom you have notified. If you fail to complete this step promptly after the Data Breach, PayPal may notify Shared Customers of the Data Breach, and will identify the Shared Customers from your PayPal Account records of who has paid you using a card.

d. If requested by PayPal, have an independent third party auditor, approved by PayPal, conduct a security audit of your Critical Systems and issue a report. You agree to comply with PayPal's request under this clause at your own expense. You must provide a copy of the auditor's report to PayPal, and PayPal may provide copies of it to the banks (including, without limitation, Acquiring Institutions) and Card Associations involved in processing card transactions for PayPal. If you do not initiate a security audit with 10 business days of PayPal's request, PayPal may conduct or obtain such an audit at your expense. See also Schedule 1 on Audit.
e. Cooperate with PayPal and follow all reasonable instructions from PayPal to avoid or mitigate consequences of the Data Breach, to improve your Critical Systems so that they satisfy the requirements this Agreement, and to help prevent future Data Breaches. However, PayPal shall not require you to do more than this Agreement requires, unless the additional measures are reasonable in light of the risk to Shared Customers and the best practices of online retailing.
f. Resume normal operation of your Critical Systems only when you have ascertained how the Data Breach occurred and taken all reasonable steps to eliminate the vulnerabilities that made the Data Breach possible or which could make other Data Breaches possible;
g. Report the Data Breach to law enforcement authorities, cooperate in any investigation that they undertake, and cooperate as the authorities may request in order to identify and apprehend the perpetrator of the Data Breach.
h. Refrain from using Card Data that have been exposed or modified in the Data Breach. However, this clause does not prevent you from obtaining and using Card Data again from Shared Customers affected by the Data Breach, after the vulnerabilities in your Critical Systems have been remedied pursuant to (f) above.

Data protection

9. **You as data controller**. You confirm that you are the data controller (as defined in the Data Protection Directive) for all personal data of Shared Customers that you collect and store.

10. **Your compliance with European privacy laws**. You agree to comply with all applicable laws and regulations, including without limitation, the laws of your country that transpose the Data Protection Directive or any successor to it and any rules or guidance by the data protection regulator of your country.

Card Data and PCI DSS

11. **Retention of Card Data**. Unless you receive and record the express consent of the cardholder, you may not retain, track, monitor or store any Card Data. You must completely and securely destroy all Card Data that you retain or hold within 24 hours after you receive an authorisation decision from the issuer relevant to that Card Data.

    If, with the cardholder's consent, you briefly retain Card Data, you may do so only to the extent that the Card Data are necessary for processing payment transactions with the cardholder's authorisation. You must never give or disclose the retained Card Data to anyone, not even as part of the sale of your business. Moreover, and regardless of anything to the contrary, you must never retain or disclose the card verification and identification data printed in the signature stripe on the back of the card (i.e. the CVV2 Data), not even with the cardholder's consent.

12. **Card Data that you must not store**. Notwithstanding the immediately preceding clause, you agree to not store any personal identification number (PIN) data, AVS Data, CVV2 Data, or data obtained from the magnetic stripe or other digital storage facility on the card (unless that data is also printed or embossed on the front of the card) of any cardholder. Card associations may impose fines if you violate this clause, which reflects card association rules. In this clause, 'store' means retain in any form, whether digital, electronic, paper-based, or otherwise, but does not include temporary capture and holding of data while it is actively being processed (but not afterwards).

13. **Merchant's use of Card Data**. You agree not to use or disclose Card Data except for the purposes of obtaining authorisation from the card issuer, completing and settling the Card Transaction for which the Card Data was given to you, together with resolving any Chargeback or Reversal Dispute, or similar issues involving Card Transactions. PayPal is required by banking laws to refund payments lacking the payer's authorisation, so your use of Card Data to carry out a Card Transaction must be authorised by the cardholder or it will subject to Reversal.

14. **Secure storage and disposal of Card Data**. You agree to:
    a. establish and maintain sufficient controls for limiting access to all records containing Card Data;

b. not sell or disclose to a third party any Card Data or any information obtained in connection with a Card Transaction;
c. keep no Card Data on paper or in portable digital storage devices such as USB memory devices or removable disks;
d. not reproduce any electronically captured signature of a cardholder except on PayPal's specific request; and
e. destroy Card Data either by destroying the medium on which the Card Data are stored or by erasing or rendering the Card Data completely and irreversibly unintelligible and meaningless.

If you transfer your business, Card Data and any information you have about Card Transactions is not transferable under Card Association rules as an asset of the business. In such cases, you agree to provide the Card Data and any transactional data to PayPal if it requests. If PayPal does not request such data, you must destroy it when your business transfers.

15. **PCI DSS audit**. If PayPal so requests, you agree that a Qualified Security Assessor may conduct a security audit of your systems, controls and facilities and issue a report to PayPal and the Associations. You agree to cooperate fully in the conduct of this audit, and to provide any information and access to your systems required by the auditor for the performance of the audit. You also agree to bear the reasonable expenses of this audit. If you fail to initiate such an audit after PayPal requests you to do so, you authorise PayPal to take such action at the Merchant's expense, or PayPal may immediately suspend your use of your Product. You will receive a copy of the audit report, and PayPal must also receive a copy and provide a copy to any Acquiring Institution or Card Association that requests a copy.