>> **View all legal agreements**

Key Payment and Service Information

Last Update: July 30, 2015

Print **Download PDF**

This description of the Service is a summary only. It does not include all definitions, exclusions, terms and conditions relating to the Service. The full terms and conditions are set out in the User Agreement that can be accessed from the footer of any page on the PayPal website. This summary does not form part of the User Agreement. This document is subject to change.

This document and the User Agreement explain information that we are required by law to communicate to you. We update it as the Service (defined below) changes.

A glossary appears at the end of this document.

PayPal Service Essentials

What is the PayPal Service?

PayPal enables individuals and businesses to send and receive electronic money online. It also provides other financial and related services. These services are collectively referred to hereafter as the "Service".

You can use the Service to make single or "one-off" payments, or you can open an account with us which will make payments easier, enable you to receive payments as well as send them, and provide more functionality and better payment records.

Who provides the Service?

The Service is provided by PayPal (Europe) S.à r.l.et Cie, S.C.A. ("**PayPal**") to registered users in the European Economic Area. For details on how to reach PayPal, please refer to **this** page on Customer Service, or in an emergency, see "**What to do**" below.

PayPal (Europe) S.à r.l. et Cie, S.C.A. (R.C.S. Luxembourg B 118 349) is duly licensed in Luxembourg as a bank (or "credit institution" in legal terms). We are under the under the prudential supervision of the Luxembourg financial regulatory authority, the Commission de Surveillance du Secteur Financier or CSSF. The CSSF maintains a register of the organisations that it regulates at **http://supervisedentities.cssf.lu/index.html?language=en#Home**. PayPal (Europe) S.àr.l .et Cie, S.C.A. is number B00000351 on the register, but you can also look us up on the register by our name.

What do you need to use the Service?

To use the PayPal Service you only need:

- A computer, smartphone (such as an Apple iPhone or an Android or Windows phone) , or tablet computer (such as an Apple iPad or Android or Windows tablet)
- A data connection to the Internet. The PayPal Service will not work if your computer is offline.

Those are the technological requirements. Obviously, the better your computer and Internet connection operate, the better the Service will operate. If your computer has a virus or other security problem, it could affect the PayPal Service along with other operations on your computer. It is best to follow all security guidance from the maker of your computer and its operating system, and to use antivirus protection if recommended for your operating system. Keep your system up to date, particularly your operating system, browser and anti-virus software. Take care when downloading from the internet: if you do not know and trust the source of your download, you take a risk that the downloaded data turns out to be harmful.

Money is what you use the PayPal Service for, so you will also need money to send or receive for PayPal to be useful. The PayPal Service will also

be more useful to you if you have a bank account, and/or a credit or debit card. The Service is a facility that lets you use those funding sources (bank and/or card) online without having to divulge the details about them except to us and the other carefully selected third parties referred to in our Privacy Policy. The Service is designed to work with your other bank accounts and your cards so that they become easier and safer to use online.

Single or "one-off" payments

If you use the Service to make a single payment (without an account with us), we will provide you with information relating to that payment both before and after you instruct us to make the payment.

This information will be made available to you:

- On the web-pages we show you before your payment is executed
- In any email we may send you, and
- In this notice of "Key Payment and Service Information"
- When using the "Payment upon Invoice" product (where available) some information may might also be sent to you by the merchant you are paying.

We do not charge you to send a single payment via the Service (although we may charge for another service such as a currency conversion).

The information that you must provide to us to make a single payment will include your credit or debit card details and other information which will be set out on the web pages where you instruct us to make the payment.

The payment will be executed as soon as the payment schemes available to PayPal allow (which can be within the next business day) after you give us your payment instruction. If the person you are sending your payment to instructs us that they wish to settle your payment at a later time, we will execute your payment order when they inform us.

Limits apply to payments that you send or receive without having an account with us. For more information, see "**Sending payments**", "**Receiving payments**" and "**Withdrawing funds**" below.

Opening a PayPal account

Individuals and businesses can open an account with PayPal. To open an account with us, a User must:

- Either be an individual (at least 18 years old) or a business that is able to form a legally binding contract; and
- Complete our sign-up process.

As part of our sign-up process, you must:

- Register an email address, which will also act as their 'User ID';
- Set a password, which we will use to log you in (see "**Keeping your account secure**" below for information on how to choose a good password); and
- Agree to our **Privacy Policy** and **User Agreement**, including the policy documents incorporated within it.

During or after the sign-up process, you can also set up a funding source in your PayPal account, which is a bank account, debit card or credit card from which we will draw funds to cover payments you make from your PayPal account.

Funding an account

The money in your PayPal account is legally termed "electronic money", which is recognised throughout the European Economic Area as a form of money suitable for use online. You can only pay funds from your PayPal account if you have funds in your account, although, if you send a payment without funds in your PayPal account to cover it, we will endeavour to obtain funds automatically from your funding sources to enable the payment to go through.

To fund an account, you must either:

- Obtain electronic money from us by paying us an equivalent amount from your funding source(s). You can do this manually using the Add Funds function available from your account interface, or we will do this automatically as needed to cover payments that you instruct us to send.
- Accept a PayPal payment that sent to you from another PayPal User.

The balance in your PayPal account represents the amount of electronic money available for paying out from your account. Electronic money is a cash-equivalent, so European law forbids paying interest on electronic money (Directive 2009/110/EC article 12).

Sending payments

To send a payment to a third party via the Service, you can either click a button on a merchant's website (or other point of sale) to pay that merchant, or if the payee has no website or button to facilitate payment, you can simply use the Send Money function in the account interface and provide the email address of the intended recipient . Either way, when you initiate the sending of money, you instruct us to transfer electronic money from your PayPal account to the PayPal account of the recipient (see also "**How do we know it's you?**" below). If the payment is accepted by the recipient (which is normally automatic), we complete the transfer.

Each new account has an initial limit on the amount of funds its user is able to send. To increase the "sending limit", the user must verify the information provided to us in connection with their account. Limits may vary at our discretion up to the maximum prescribed by laws against money laundering, but we do not provide a facility for you to vary the sending limit. The type of information required for the verification process varies depending on where you live and the type of account (personal or business) that you have. PayPal will prompt you to verify your account information and explain how to do so.

Receiving payments

Once you have opened your PayPal account, you can receive a payment via the Service by accepting a payment from another user. Acceptance is almost always automatic; you normally need not do anything to accept a payment.

The recipient is able to refund payments or, in some circumstances, to use the Service to refuse payments that have been sent by another user.

If your PayPal account is new, laws for prevention of money laundering require that PayPal limit the amount of money you can receive until you complete the verification process for your account. PayPal will ask you to verify your account and explain how to do that shortly after you open your new account.

PayPal blocks payments that appear to us to have serious security problems or to be fraudulent (see User Agreement sections 9 and 10). Sometimes, rather than blocking, we delay a payment in order to investigate it further. If we discover a fraud after you receive a payment, we ordinarily reverse the payment back to the person who was defrauded and note the reversal in your account. Sometimes we are not legally permitted to explain the blocked or delayed payment or give details about a reversal in order to avoid tipping off someone who appears to be committing fraud or other crime. Although we may have limits on what we can disclose, you are welcome to ask about blocked, delayed or reversed payments using the Secure Messaging Centre, which is described under "Communicating with you" below.

Currencies

You can send or receive a payment in a variety of currencies, including: Pound Sterling, Euro, US Dollar, Canadian Dollar, Japanese Yen, Australian Dollar, Swiss Franc, Norwegian Kroner, Swedish Krona, Danish Krone, Polish Zloty, Hungarian Forint, Czech Koruna, Singapore Dollar, Hong Kong Dollar, New Zealand Dollar, Israeli New Shekel, Mexican Peso; Argentine Peso, Brazilian Real, Philippine Peso, Thai Baht, and Taiwan New Dollar.

If you do not have a balance in the currency that you are sending, or if you withdraw a currency that does not match the nationality of the bank account receiving the withdrawal, the Service will ordinarily convert the funds into the currency of the payment you are sending or the bank account receiving the withdrawal, and will charge a fee for the conversion.

You can receive money in any of the currencies that the Service supports (listed above). If the currency you receive does not match the nationality of your PayPal account, the Service will not convert the foreign currency into the national one until you instruct it to do so, withdraw the funds into your bank account, or send them in another currency.

Before the Service converts a currency, it will inform you of the exchange rate to be applied and the fee to be charged. Once you are informed, the Service will proceed with the conversion only if you instruct it to continue.

Risk of chargeback or reversal of a payment

If a recipient does not qualify for Seller Protection (see below) and receives a payment that becomes subject to a chargeback or is reversed, the recipient (not PayPal in most cases), will be liable for the amount of that payment together with any fees such as the feee for processing a chargeback.

A chargeback is a dispute between the recipient of a card-funded payment, the bank that issued that card, and that issuer's customer, the sender of the payment. PayPal does not decide chargeback issues, and we and the payee must accept the decision of the issuing bank as final and legally binding in connection with a chargeback dispute.

Seller Protection

Under certain circumstances, PayPal will cover the loss caused by a chargeback or reversal, rather than require the recipient of the payment to reimburse it, if the payer denies having authorised the payment or claims that they did not receive the item that they paid for..

Seller Protection is available and can be claimed when the payment is listed as "Seller Protection Policy Eligible" on the User's Transaction Details page. Seller Protection eligibility depends on the following factors:

- The type of goods purchased (for example, they must be tangible, not digital);
- The countries in which the buyer and seller reside;
- The account type of the seller;
- The postal address to which the seller sends the goods;
- Evidence of the delivery method used;
- The time at which the goods were sent following receipt of payment;
- The number of accounts from which payment was made;
- The co-operation of the seller.

Buyer Protection

Buyer Protection lets buyers of eligible goods and services recover all or part of their PayPal payment for those purchases, if they were not delivered or are significantly not as the seller described them.

To receive Buyer Protection, you must file a claim, and time limits apply. The User Agreement has details on how to claim.

Withdrawing funds (redeeming electronic money)

If your account has a positive balance, you can instruct us at any time to withdraw funds from your account into a bank account registered as a funding source in your PayPal account (or, rarely, to a card funding source). Such an instruction is normally given by using the withdrawal functionality in the account interface. In legal terms, a withdrawal from a PayPal account into a bank account is a 'redemption' of electronic money.

Under normal circumstances, we will complete the withdrawal from your account within 1 business day following the completion of any checks that are reasonably required by us to prevent money laundering and fraud or to confirm your identity and your access to the bank account used for withdrawal.

If your PayPal account is new, laws for prevention of money laundering require PayPal to limit the amount you can withdraw. You can lift the limit by completing the verification process for your new account. PayPal will ask you to complete that process and explain how to do so shortly after you open your new account.

You can keep funds in your PayPal account as long as you wish. We do not charge for keeping your money in PayPal, but we also do not pay interest because interest on electronic money is prohibited.

Fees

PayPal does not charge for sending money via the Service (unless a currency conversion is required, or the payment is sent via our MassPay service, or if a sender opts to pay the fee for sending a "person to person" payment).

PayPal charges fees when certain events occur, such as:

- Receiving funds (rates vary depending e.g. on the location of the sender and recipient);
- Converting currencies (see Currencies above);
- Processing a chargeback by the sender of a payment you receive;
- Carrying out a withdrawal of funds (in some countries);
- Using certain optional services such as Mass Pay or PayPal Credit

The details of our fees can be found at the end of the User Agreement.

Closing an account or restricting its use

Either we or the account holder may close an account at any time. PayPal rarely closes accounts except where the account holder has violated

their agreement with us, and we notify an account holder before closing the account. See section 7 of the User Agreement for information on how to close your account and what effect that will have.

We may also prevent your account from sending or receiving payments, and/or from making withdrawals in certain circumstances, such as where information given to us appears to be inaccurate, you fail to perform key obligations, or you appear to have financial difficulties (see also sections 9 and 10 of the User Agreement). PayPal does not include a facility that will let you restrict or disable use of your account other than by closing it.

If we restrict your account (without closing it entirely), the Secure Messaging Centre will remain available to you after you log in, or you can reach Customer Service by telephone. You are welcome to enquire about the restriction, and we will explain the basis for it (if allowed) and how you can have the restriction removed.

PayPal may also block a specific payment (without closing or restricting the account); see "**Receiving payments**" above for more information.

Prohibited or restricted activities

We do not allow the Service to be used for the processing of payments associated with illegal activities or other activities that violate our Acceptable Use Policy.

We may also restrict the use of the PayPal service and/or refuse to carry out your payment order if this would amount to a Restricted Activity as set out in our User Agreement.

Communicating with you

PayPal will communicate with you in the following ways (among other common ways such as telephone for customer service and this website):

- **By email**, if the information communicated is not sensitive for security reasons. For example, we use email to notify you of payments sent or a change in your account settings. These email notices are usually routine confirmations of action you have taken, but if you did not take the action notified, then you must act immediately, and not be sending a reply email. See "**What to do in case of a security problem**" below if you suspect unauthorised usage of your account.
  Besides confirmation of actions taken, we use emails to get your attention (such as when you have a payment awaiting your acceptance, or a card set up in your account is about to expire) and for general announcements to all users such as updates to our online agreements. We keep confidential information in emails to a minimum because email is not a highly secure means of communication. To communicate with us securely, use the Secure Messaging Centre.
  A reply to one of our automatic emails will not get the attention from us that we will want to give to a message from you. If you must reply, please use the Secure Messaging Centre to react to an emailed notification from us, or to confirm the authenticity of an email from us.
- **By notifications on your smartphone or tablet computer**, if the settings on your device permit us to give you these notifications. These notifications serve the same purposes as the email notifications described above and let you discover unauthorised usage of your account. See "**What to do in case of a security problem**" below if you suspect unauthorised usage.
- **By the Secure Messaging Centre**, which you can access from your account, but only after you log in to your account. Because you log in, we can be more certain that we are communicating with you through the Secure Messaging Centre, so we use it for information about the security of the Service, confidential information, and other information for which security is important. However, because you must log in to access the Secure Messaging Centre, it can be less effective than email at getting your attention, so we may use an email with few details to advise that you check the Secure Messaging Centre.

This is not an exhaustive list; for example, if you telephone our Customer Service, then of course that communication will be by telephone.

We communicate with you in the language of your country. We ask you for your country when you sign up for the Service.

Resolving disputes

We will endeavour to resolve any dispute relating to the Service via our Resolution Centre, which you can access by logging in to your account. You can initiate a dispute, or respond to a dispute raised by another user, in the Resolution Centre, where you can also find help on how to use the Resolution Centre. Deadlines apply in resolving disputes so it is important to note when further action is due.

If the outcome of the dispute, after completing the process in the Resolution Centre, is not to your satisfaction, you may complain to the Financial Ombudsman Service (if you are a UK resident User) or to the **European Consumer Centre (ECC-Net)**, or you can sue us in the courts of England and Wales (or your local court if you are a consumer). You may also refer an unresolved dispute in writing to our regulator, the CSSF at the following address: Commission de Surveillance du Secteur Financier (CSSF) 110, Route d'Arlon L-2991 Luxembourg.

Which law applies

The legal relationship with you is governed by the laws of England and Wales.

Secure use of our Service

From a consumer's perspective, PayPal's basic product is the Service, which is often compared to a wallet, a safe place for keeping cash, cards, and other means of payment. Security is a major reason why a wallet is good to have: the PayPal Service saves you from having to disclose to online sellers the details for accessing your cash, so the people you pay do not get access to your means of payment (card details, bank account details).

Besides security, part of a wallet's utility also lies in it being ready and convenient: a wallet is not a safe but something to hand and easily opened when you need cash. The balance between security and ready convenience is difficult to strike: we avoid inconveniencing you when a security check would add little value, but when the risk (amount at stake, likelihood of loss) is higher, we must ask you to help us and protect yourself as we ensure that we are dealing with you and not an imposter. We make the most of less intrusive means of recognising you from your behaviour, but sometimes we must also ask you to demonstrate that the person doing something with your account really is you.

How do we know it is you?

When you send a payment, we need to confirm that it is you, our account holder, who is instructing us to pay. We will deduct the payment from your account, so confirmation that it is really you consenting to the payment ensures that we deduct from your account only payments that you told us to make. Besides payment instructions, for other operations involving your money or your PayPal account settings, we confirm that it is you performing the operation.

Logging in with your login credentials (including password or PIN) gives us basic assurance that you are the person logging in. The security of this basic method depends on whether you maintain the secrecy of your login credentials, especially your password and PIN. If you disclose your login credentials, you give up control over your PayPal account. If you wish to let someone else use your account, do not share your login credentials but instead create a separate user and login capability for the other person (log in, then under "Profile and settings", choose "Manage Users"). Never divulge your own login credentials to anyone so that you always retain control over your account. See "**What to do**" below if you think your login credentials may no longer be known only to you.

A PayPal representative will never ask you for your password or PIN; they are recorded in encrypted form in our system and are not accessible to PayPal staff. Do not disclose your password or PIN to PayPal staff or anyone else. If you forget your password, we will change it to a temporary one known to you and us, but you will need to change the temporary password as soon as you use it for the first time. You can change your PIN yourself from your account Profile, once you log in with your password.

European laws on the security of internet payments require more than the basic level of assurance (provided through login) for certain activities. PayPal may ask you for further assurance that you are the person performing an activity involving your money or account setup. For example, if you are sending a large payment funded by a card, PayPal may ask you to log in with your card issuer using 3D Secure in order to demonstrate that your card issuer recognises you as the holder of your card. Sometimes we obtain further assurance less obtrusively such as by checking that the device that you are using is one that we associate with you. To dissociate yourself from a device, "Unlink" it from you by logging in, then under "Profile and settings" choose "Phone".

Although we sometimes use stronger than basic confirmation of your identity, PayPal will continue accepting the basic level of assurance (login with your email address and password) for certain low-risk transactions. In evaluating whether a transaction is low risk, we consider the amount at stake as well as whether the transaction fits your apparent habits as revealed in your account history. For example, we are more likely to consider a transaction low-risk if you have spent money with the same payee before and recently, if you are sending from a device and/or location common for you, or if in other ways the transaction fits the patterns of your payment activity.

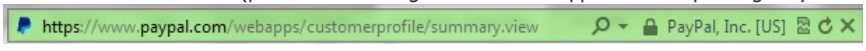
How do you know it is us?

PayPal works diligently to stop others from counterfeiting our website, mobile phone apps, and other means of accessing our Service. However, our work to eliminate imitations is never 100% successful: someone can impersonate PayPal until we catch up with them. If you think a fake website is PayPal's real website, you may log in at the fake one, and thereby disclose your login credentials to a PayPal imposter. See "**What to do in case of a security problem**" below if this has happened to you.

To help ensure that you log in to the real PayPal website:

- **Avoid using a link to the PayPal website**. The linking code that takes you from a reference to the referenced website is not visible to you, so in following a link, you do not actually know for certain where you are going. Following a link is safe only if you can trust the linker, and you may not always know who that is. Emails can be made to look as if they come from PayPal, when really they do not, so avoid using links in emails to access PayPal. Links on websites whose authors you do not know and trust can also lead you to imitation websites. The easiest way to be sure you go to the real PayPal website is to type "paypal.com" in the address bar of your browser and hit Enter.

- **Check the address bar**. When you reach what looks like the PayPal website, check the address bar at the top of your browser window. It should look about like this (please allow for slight variations in appearance depending on your browser):

  In that example, "https" and the closed padlock indicate that the connection between your browser and the PayPal server is encrypted, so others along the way cannot eavesdrop. The words "paypal.com" and "PayPal, Inc." confirm that your browser is connected to our server,

and the green shading indicates that the browser "knows" it is us because of a certificate issued by a trustworthy third party who identified us using standard methods. If the address bar is yellow or red, or if the connection is not secure (padlock open or no "https") or connected to us (address is not to paypal.com), do not log in there. Fraudsters may misuse our name, but it is more difficult for them to misuse our internet domain name, paypal.com, so look for that domain in the address (exactly "paypal.com" just before the first slash appears).

When you instruct us to make a payment for you, you are usually at the website of the merchant that you intend to pay. To instruct us to pay, we normally ask you to log in (so that we know it is you instructing us), so the merchant's website will redirect you to a PayPal window for login. You can always check the address of that login window to ensure that the merchant's website has redirected you to us. Note that when you are redirected to us from a merchant in this manner, the merchant's name will also appear, not because you are still on the merchant's website, but to help you maintain the context: you are buying something from the merchant, and the payment step in that process takes you to us momentarily, but you will return to the merchant after paying.

To ensure that the PayPal app on your mobile phone is authentic and comes from us, obtain it from a trustworthy source such as the Apple App Store or Google Play.

Some PayPal customers let you log in to their websites using your PayPal login credentials; this can save you from having to create an account on the website in order to use it. However, although you use your PayPal login credentials and PayPal handles the login process, you are not logging in to PayPal but rather to the third party's website. If you log in (or attempt to log in) to the third-party website using your PayPal login credentials, PayPal will inform the third party when you successfully log in or when an attempt fails, but PayPal does not share further information with the third party without first obtaining your consent.

Keeping your account and money secure

To prevent loss, it is important that you do all you can to maintain control of your PayPal account. You lose control over your account if you disclose your login credentials, particularly your password and PIN. There are no circumstances in which disclosure of your password or PIN is justified. PayPal accounts are meant to belong to one person only. We do not support joint accounts or multiple account holders, so the money in your account is yours alone as far as we are concerned. If you want someone else to use your account, create a new user for your account (besides yourself) so that the other person does not log in with your password (to create a new user, first log in, then under "Profile and settings", click on "Manage users"). Never disclose your password to another person, and if you do, change your password immediately (log in, then under "Profile and settings", click on "Change password"). Never disclose your PIN either, and change it immediately if you do. See below under "**What makes a password good?**" for advice on password selection and the **similar section on PIN selection**.

Besides your password, PayPal also confirms your identity by means such as the following:

- **3D Secure**: Card issuers operate their own login facilities called 3D Secure to confirm that the person using a card is indeed the card holder known to the card issuer. PayPal uses 3D Secure logins to doubleIcheck that it is you taking an action, when you have a card included among the funding sources for your PayPal account. Because re-using passwords reduces their security, it is best to use a different password for 3D Secure, not the same password that you use for PayPal. For a Visa card, 3D Secure is also known as Verified by Visa, and for a MasterCard, as MasterCard SecureCode. If you forget or lose the password that you use for 3D Secure, please contact your card issuer immediately. PayPal uses but does not manage 3D Secure, so your card issuer can help with a 3D Secure password problem but PayPal cannot.

- **Your devices**. We can readily identify a particular smartphone (an Apple, Android, Windows or similar mobile phone). Because a mobile phone generally has only one main user, we use your phone as a way of confirming that you are the person taking a certain action. When you are using PayPal from one of our mobile phone apps, we can confirm in the background that you are using your phone to access your account. If you should lose a device that we use to identify you, please break your link with that device by logging in, then under "Profile and settings", click on "Phone" and then on "Unlink" to dissociate yourself from that phone.

  We also identify the computer from which you are logging in, but because people often share computers, we do not view a computer that you frequently use as a specific identifier for you but rather a corroborating one.Which computer you are using, your location, where you spend, and other behavioural characteristics of your PayPal usage help us identify you, but none of these additional identifying characteristics is conclusive in itself.

- **Your appearance**. If you use PayPal on a smartphone, the PayPal app will ask you to take a selfie, a photo of yourself made using your phone. To take the photo, you must be logged in on the phone that you use to take the photo. You can try again, if you do not like the first photo, but you cannot upload a favourite photo from an external source. When you use PayPal in a physical shop, the cashier taking your PayPal payment can refer to your PayPal photo to confirm that the account holder and you are the same person.

PayPal is leading innovation in developing new ways of confirming who is using our Service, without increasing our reliance on passwords and PINs. We have led formation of the FIDO Alliance, which works to reduce reliance on passwords across the technology industry by developing standardised alternatives. We will continue innovating and strengthening our ability to recognise you when you use our Service.

What makes a password good?

Passwords vary in how easy they are to guess. The best guesswork is done by computers these days, which can try many thousands of character combinations per second, and guessing algorithms often start with the combinations that people are most likely to choose. To guard against guessing, PayPal limits the number of tries within a given time, but we cannot fully eliminate the potential for guessing without also making login more difficult for you.

The best protection against guessing is to choose a password which is:

- **Nonsensical**: If you choose only from words in a dictionary, then you limit the range of possibilities to a small subset of the total combinations available, making your password an easy guess for a program that can try the entire contents of a dictionary in a few minutes.
- **Non-phonetic**: You also limit the range of possibilities if you make your password pronounceable. A good password will be a random combination that makes full use of the entire character set.
- **From a large character set**: Include all the different sorts of characters on your keyboard rather than just one or two sorts. The larger the range of characters, the larger the number of possible passwords and the harder your password will be to guess.
- **Long**: The number of possible combinations increases exponentially with each character you add to your password, although the difficulty of remembering and entering your password also increases with length. A password of 10 random characters is probably not too bad, but if the sequence of characters is not completely random, then a longer one is advisable.
- **New**: Re-using passwords or parts of passwords undermines the benefit of changing your password. If you use the same password for different services, one cracked password will allow access to all the different services. You can address the challenge of remembering passwords better through software (see below) than by taking the risk of weak passwords.

When you enter a new password, PayPal will give you feedback on its strength, and you will protect yourself better if you act on this feedback. We will not accept too weak a password. Never use a website to generate a password for you; the website can follow you and note where you enter that password.

Long, nonsensical, non-phonetic passwords tend to be difficult to remember. If you are not good at memorising, it is better to write down your password than to forget it, but then you must secure the place where you keep the writing. Instead of a physical place (where you may not always be when you use PayPal), software products are available for securing passwords. You can find those products by searching the internet for "password security software" or the like. Choose the product carefully because you will be entrusting your passwords to it.

Your browser can probably also remember your passwords for you, but controlling access to your browser and the passwords in it is likely to be more difficult than controlling access to specialised password security software. Your browser is accessible to the websites you visit and to others who use your computer, but more specialised software can be less externally visible and accessible. Specialised software will require you to identify yourself to it (such as by logging in or providing a physical token), but a browser often does not, leaving passwords stored in a browser exposed to later unidentified users.

What makes a PIN good?

A PIN (personal identification number) is never as good as a good password because its character set is drastically limited to only ten numerals (0-9), and a PIN is often shorter than a password. PayPal requires a password, not a PIN, unless you are logging in from a PayPal app installed on your mobile phone. Although you may use your phone number and PIN to log in from your phone, you also have the safer option of using a password instead. We will treat your login as less reliable if done with a PIN from a phone that we do not recognise as yours. We list your phones in your account Profile, and you can "unlink" a phone from you if it ceases to be yours.

A good PIN is long and random. A four-digit PIN requires trying at most only 10,000 combinations to achieve a successful guess; adding just one more digit raises the possible combinations to 100,000. Avoid predictable sequences such as "12345" or "36987" which on an ordinary keypad is simply down the right side then over across the bottom row.

What to do in case of a security problem

If you suspect a security problem, act on it immediately but without panic. Delaying may worsen the consequences. Calling customer service is ***not*** the first action you should take.

First, ask yourself which of the following best describes the problem:

a. I can log in. Someone else is or may be using my account, or my login credentials may no longer be secret.

b. I can log in and I think my login credentials are safe, but unauthorised activity appears to have occurred in my account.

c. I can't log in. Someone else is or may be using my account.

The subheadings below deal with these situations.

"I can log in but..."

If you can still log in to your PayPal account, but you suspect that someone else may be using your account, or unauthorised activity appears to be occurring, the first thing to do is to log in and change your password, even if you have no reason to believe that someone else may have discovered your password. Fraudsters often have password-guessing programs, so the best way to be sure nobody knows your password is to change it. You can change your password much more quickly than we can, if you can still log in.

To change your password, you must first log in. Then click on "Profile and settings", and under "Password", click Change. See above under "**What makes a password good?**" for advice on how to select a strong password. When you change a password, we secure the communication channel between you and our servers, so changing a password is generally a secure process and you need not worry that someone is eavesdropping. Select your new password carefully and avoid any resemblance to the old one.

After you have changed your password and logged in again, please confirm which activity appears to be unauthorised. There is a significant difference between "I don't remember making that payment" and "I know I didn't do that payment because I have never heard of Millie's Handbags, I'm a bloke, and I don't use a handbag." Please do not report a payment as unauthorised unless you are sure that you did not authorise it. Intentionally and falsely reporting a payment as unauthorised can amount to fraud.

If you are sure that unauthorised activity has occurred, please report that to PayPal by contacting Customer Service (details below). However, report the unauthorised activity only after you have changed your password: changing your password regains your control over your account and is an essential first step, before sorting out the consequences of a loss of control.

"I can't log in"

If you can no longer log in to your PayPal account, please request a password reset by calling Customer Service (email is not useful for password resets because it is not very secure). Request a reset urgently, if you suspect that an unauthorised person may be using your account. The request is less urgent if it is unlikely that anyone else can access your account.

Contacting Customer Service to reset your password

If you can still log in, then you can solve your most immediate problem faster than we can; see "**I can log in but...**" above. If you cannot log in or you have already taken what action you can, then call Customer Service (details can be accessed at the bottom of this page).

If you can log in, please do so, click "Need Help?" near the bottom of the web page, and note down the one-off passcode that you will be given. If you cannot log in, please explain why not when the customer service representative asks for the passcode.

If you can still log in, you can use the Secure Messaging Centre to contact us instead of telephoning. However, if you urgently require a password reset that you can't do for yourself, please call us for the fastest possible action. You can also use the Secure Messaging Centre to address the consequences of intrusion into your account such as payments you did not authorise, or to obtain customer service for other issues.

When you request a password reset, we must ensure that it is you who is changing the password on your account. We do that by asking you certain questions whose answers only you are likely to know. If you change your password online through our Help pages, the questions will be the ones you selected and answered when setting up your account. Those questions can be seen from your account profile, and you can choose new ones if you wish.

Losses due to unauthorised usage

Losses are best prevented, which you can do by **keeping your account secure** and **acting immediately if a security problem occurs**. In many situations, you rather than PayPal are in the best position to prevent loss.

PayPal will not hold you responsible for any unauthorised use of your account by a third person, provided that we are satisfied that you have taken reasonable care to protect the security your account.. and you have informed us of the unauthorised use in a timely manner.

More security information

The **PayPal Security Centre** has more information on security and our policies relating to it.

Glossary

3D Secure: A process prescribed by card associations (such as Visa and MasterCard) to enable a card issuer to confirm the identity of a person using a card issued by that issuer. 3D Secure uses a password recognised by the issuer (not PayPal) to confirm that the person entering the password is the card holder known to the issuer. 3D Secure is a generic term; Verified by Visa and MasterCard SecureCode are trade names for 3D Secure.

Login credentials: The data that you use to log in, such as your email address and password, or (on a mobile phone) your phone number and PIN. Your email address and phone number may be known in other contexts besides login, but your password and PIN must be secret to protect your account from unauthorised access.

Secure Messaging Centre: A means for you and PayPal to communicate with each other in a manner similar to email, but with greater confidentiality and security. You must log in to PayPal to use the Secure Messaging Centre.

We: PayPal (Europe) S.à r.l. et Cie, S.C.A., the provider of the Service, as explained in "**Who provides the Service?**" above.

You: The rightful holder of a PayPal account set up in your real name.

For more information, you can:

- Refer to our **Help service**
- Call **Customer Service**

Finally, just so you know:

- **Our guidelines for your "Secure Use of Our Service" are what we reasonably believe to be best practice but are not exhaustive and do not constitute advice of any kind. Prevalent technologies, associated risks and your specific circumstances constantly change, so we provide those guidelines with no warranties, representations and guarantees (to the extent allowed by applicable law and subject to the PayPal User Agreement). Always do your own research on top and seek individual professional advice if you want to ensure that what you do is right for your specific circumstances.**
- **The above information does not constitute an endorsement or recommendation of any third party products or third party services of any kind.**
- **Where we link to other websites, we can't be responsible for their content.**