Customer Security and Fraud Awareness

Website Communication

Customer Security and Fraud Awareness

Website Communication

Our Approach to Security

When it comes to your financial information, your security is our top priority and when you access your account, it is important that we know it is you. Here are some of the ways we do that:

Login Details – we provide you account login details unique to you, to protect yourself we recommend you do not share them.

Login Process – Two Factor Authentication provides an additional layer of security to your account. It requires two successive factors of authentication:

- 'something you know' such as your account number and password, and
- 'something you have' such as your mobile device.

Account Questions – If you contact our customer services team, we will ask you to confirm your identity by asking you questions related to your account.

One Time Passcodes or push messages – We may send unique one time use codes or push messages to your registered devices when additional security and validation is required, for example:

- You make payments from your online account;
- Periodically at login just to make sure it is you;
- When you request to make changes to your personal details; or
- When you contact our customer services team.

Providing Information – we will never ask you for your password details or PIN number.

If we suspect that fraudulent activity may have taken place across your account we may temporarily Block your account and contact you for further information. We will contact you in accordance with your Communication preferences saved on your account which may include email, telephone and in app PUSH message.

How to Report Fraud

If you notice something suspicious and believe it could be fraudulent, you should contact us as soon as you become aware of it.

Reporting Fraud: Please contact customer services: cards@vfxplc.com or call +44 207 959 6995

Lost or Stolen Cards: Immediately Block your card by logging onto your online account and then report to customer services.

Suspicious Emails: Please contact customer services.

How to Protect Yourself from Fraud

Help to keep yourself safe from fraudsters by following the tips below. Remember, if you are ever unsure, do not act.

Always make sure your mobile telephone number and email address registered with us is up to date, we will use these to contact you if we notice unusual activity on your e-money account.

Some Tips for Using Your Account Safely

When accessing your account online:

- Use up to date antivirus software and firewall.
- Make sure you keep your computer and browser up to date.
- Use secure networks, a guest wireless network such as a hotel may not be secure.
- Use strong passwords and change them regularly.
- Don't share any passwords including one-time passwords sent to you.

When using a mobile application

- Only install apps from recognised app stores.
- Consider the app ratings and reviews.
- Be aware of what permissions you are granting.
- Treat your phone as your wallet.

When shopping online

- When using an online retailer for the first time, do some research to make sure that they are genuine.
- Do not reply to unsolicited emails from companies you don't recognise.
- Before entering your prepaid card details, make sure the link is secure. There should be a padlock symbol in the browser frame window which appears when you login or register, if this appears on the page rather than the browser it may indicate a fraudulent website. The web address should begin with https://, the 's' stands for secure.
- Always log out of website after use. Simply closing your browser is not enough to ensure your data is safe.
- Keep your PIN safe and do not share it.
- When entering your PIN, check for people around you and hide your PIN number.
- Always check your statements.

Remember, if you decide to donate, resell or recycle an old mobile phone, computer, laptop or tablet, make sure you fully remove all data and apps first as otherwise these may be accessed by whoever your device is passed to.