Fraud Information for Customers

It is possible that at some point you may become a victim of Fraud, at NBEUK we wish to ensure that **all** of our customers are supported in not only trying to prevent fraud but also in what actions to take should you become a victim of fraud.

There are many different ways that you can become of a victim of fraud, whether it be by impersonation, or an Authorised Push Payment Fraud.

Identity Theft & Impersonation Fraud

Identity fraud, or 'ID theft', involves the use of a person's stolen details to commit crime. Many victims never find out exactly how someone got hold of their details.

If you start getting post for someone you do not know, try to find out why.

Lenders use the electoral roll to check who is registered as living at a particular address.

When registering to vote, tick the box to opt out of the 'edited' register. This will help prevent unsolicited marketing mail or junk mail. This does not affect credit checks.

You can also:

- sign up to the Mail Preference Service to prevent marketing letters
- protect mail left in communal areas of residential properties
- redirect your mail when moving home

Be extremely wary of unsolicited phone calls, letters or emails from your bank or other financial institution asking you to confirm your:

- personal details
- passwords
- security numbers

Regularly check your bank accounts and chase up any statements that you don't get when you expect them.

APP Fraud

Authorised push payment fraud is one of the fastest growing types of scam around.

APP fraud involves the fraudster tricking their victims into willingly making bank transfers to them.

They often pose as somebody from the bank purporting that the customer has been a victim of fraud and will need to transfer money over to another account, or quite often purport to be conveyances or builders.

Often the fraudster has access to customer data usually by hacking e-mails and asking for payments to be diverted to other accounts.

How to Avoid APP Fraud

If you receive an e-mail or a phone call asking you to divert money into a differing account, question it to the highest level. If the fraudster purports to be your conveyancer or builder, contact them on the usual channels not the e-mail address or using contact details on the suspect e-mail.

If somebody purports to be from your bank requesting you to move money, arrange to the call back but call on a known publically available number for the bank.

Most Important **Never** rush a payment, genuine organisations don't mind waiting.

What should you do if you believe you have been a victim of fraud.

Please feel free to contact the Bank, we may be able to liase with other financial institutions in an attempt to recover your money (recovery is not guaranteed). We can ensure additional safeguards are placed on your account to prevent future frauds.

You may also wish to contact CIFAS, who can help place markers on your data to help prevent future frauds.