INVOICE FRAUD:

Barclays Bank plc has been receiving numerous complaints from individuals who are not customers of the bank stating that funds/payments due to them have been fraudulently moved into accounts with Barclays Bank in the UK. These individuals have requested us to intervene and block the said accounts so that their funds/payments can be recovered.

While there is little that Barclays Bank can do to stop such fraud, we would appeal to you to be vigilant at all times to avoid becoming a victim. We detail below the modus operandi and the Do's and Don'ts that one should abide by.

How it works: Fraudsters hack into the e-mail accounts of self-employed businessmen while at the same time creating similar looking e-mail accounts. So, for e.g., if the e-mail account hacked into is widget@abcd.com, the fraudster at the same time creates another e-mail account that looks similar – widget@abcd.in

The fraudster then utilises the information on transactions, deals etc that he is able to access by virtue of having hacked into the self-employed businessman's account and writes to clients from the e-mail ID he has created. He requests them to divert payments to a Barclays account in the UK instead of the bank account he had previously communicated to them. The reasons typically cited are audit issues, tax enquiries, etc.

The moment the client transfers the funds into the Barclays UK account, the money is immediately either withdrawn or electronically transferred to another account in another geography/jurisdiction. This is done to make litigation/recovery all the more difficult.

What you can do to spot this fraud:

- Counterfeit invoices normally never stand up to scrutiny. If you suspect the authenticity of an invoice, always compare it with a genuine one. You'd be able to tell the difference.
- Compare the contact numbers and e-mail addresses of the company with those that you have on record. The contact e-mail address may only have a minor difference, giving one the impression that it is genuine. For e.g., it will look almost identical to the original e-mail address but may read ".org" or ".in" instead of ".com" or ".co.uk".

What you can do to reduce the risk of being a victim of this scam:

- Always confirm change of bank account information with the company making the change. Use the contact details you have on record rather than that provided in the letter informing of the change.

- Set up designated single points of contact with companies that you make regular payments to. This could be a person or a department that you are in regular contact with to raise any issues/concerns.
- For staff that handle invoices, ensure that they look out for any irregularities, including change of name, amount or address.
- When making a payment against an invoice, always send an e-mail to the company using the contact information you have on record, letting them know that you've paid them and also provide the bank details that you have credited.
- Fraudsters will check on your website to identify your suppliers of goods and services. Consider if it's necessary to even publish this information.
- When a large payment needs to be made, consider setting up a meeting with the company involved to ensure that the payment is being made to the correct bank account and recipient.