CLAIMS:

1. An electronic method of fraud prevention at a host system, the method comprising:

receiving, at the host system, a request to purchase one or more digital products from a user device of a user,

receiving, at the host system, a request to settle the purchase by an Internet bank transfer from a bank account of a bank;

connecting, with the host system, the user device to a third party system to enable the user to attempt to settle the purchase by making the Internet bank transfer from the bank account;

monitoring, at the host system, the attempt to settle the purchase by an Internet bank transfer from the bank account to determine whether it is indicative of an unacceptable fraud risk of a transaction by:

receiving, from the user device, data associated with the user device;

processing the received data to assess a fraud risk of the transaction;

terminating, with the host system, the transaction without releasing the requested one or more digital products in response to determining that the fraud risk is unacceptable based on the processing of the received data;

receiving, from the third party system, an identifier unique to the bank account; and

processing, with the host system, the received identifier to assess the fraud risk of the transaction, the processing of the received identifier including determining whether any prior transactions associated with the received identifier are indicative of the unacceptable fraud risk;

terminating, with the host system, the transaction without releasing the requested one or more

digital products in response to determining that the fraud risk is unacceptable; and

accepting, with the host system, the payment and releasing the requested one or more digital products in response to determining that the fraud risk is acceptable based on the processing of the received data and the processing of the received identifier,

wherein the data associated with the user device includes data that is dependent on a current status of the user device.

2. The method as claimed in claim 1, wherein the third party system is configured to enable the user to specify details of the Internet bank transfer.

3. The method as claimed in claim 1 or claim 2, wherein the third party system enables the user to select a bank account from which funds are to be transferred by Internet bank transfer.

4. The method as claimed in any one of claims 1 to 3, wherein the identifier is unique to the bank account but does not allow the host system to identify the bank account.

5. The method as claimed in any one of claims 1 to 4, wherein monitoring the attempt to settle the purchase comprises monitoring completion of at least one web form to determine whether a manner of completion of the at least one web form is indicative of the at least one web form not being completed by a human user.

6. The method as claimed in any one of claims 1 to 5, wherein the digital product is a mobile device recharge voucher.

7. The method as claimed in any one of claims 1 to

6, wherein the data that is dependent on the current status of the user device comprises either or both of a location of the user device and an IP address from which the request was received from the user device.

8. A host system for fraud prevention, the host system comprising:

a purchase request receiver configured to receive a request to purchase one or more digital products from a user device of a user,

a payment module configured to receive a request to settle the purchase by an Internet bank transfer from a bank account of a bank, the payment module configured to connect the user device to a third party system associated with a bank to thereby enable the user to attempt to settle the purchase by making the Internet bank transfer from the bank account;

a transaction monitor configured to monitor the attempt to settle the purchase by an Internet bank transfer from the bank account to determine whether it is indicative of an unacceptable fraud risk of a transaction by:

receiving, from the user device, data associated with the user device;

processing the received data to assess a fraud risk of the transaction;

terminating, with the host system, the transaction without releasing the requested one or more digital products in response to determining that the fraud risk is unacceptable based on the processing of the received data;

receiving, from the third party system, an identifier unique to the bank account; and

processing the received identifier to assess the fraud risk of the transaction, the processing of the received identifier including determining whether any prior transactions associated with the received

identifier are indicative of the unacceptable fraud risk; and

a transaction terminator configured to terminate the transaction without releasing the requested one or more digital products in response to determining that the fraud risk is unacceptable,

wherein the host system is arranged to accept the payment and release the requested one or more digital products in response to determining that the fraud risk is acceptable based on the processing of the received data and the processing of the received identifier,

wherein the data associated with the user device includes data that is dependent on a current status of the user device.

9. The host system as claimed in claim 8, wherein the third party system is configured to enable the user to specify details of the Internet bank transfer.

10. The host system as claimed in claim 8 or claim 9, wherein the third party system enables the user to select a bank account from which funds are to be transferred by Internet bank transfer.

11. The host system as claimed in any one of claims 8 to 10, wherein the identifier is unique to the bank account but does not allow the host system to identify the bank account.

12. The host system as claimed in any one of claims 8 to 11, wherein the transaction monitor is configured to monitor the attempt to settle the purchase by monitoring completion of at least one web form to determine whether a manner of completion of the at least one web form is indicative of the at least one web form not being completed by a human user.

13. The host system as claimed in any one of claims 8 to 12, wherein the data that is dependent on the current status of the user device comprises either or both of a location of the user device and an IP address from which the request was received from the user device.

14. The host system as claimed in any one of claims 8 to 13, wherein the digital product is a mobile device recharge voucher.

15. Computer program code which when executed implements the method of any one of claims 1 to 7.

16. A tangible computer readable medium comprising the computer program code of claim 15.