

Likewise, alternative biometric inputs may be susceptible to similar fraudulent exploitation. By way of example, in a voice recognition system, a user may register a recording of their speaking their name on a database for subsequent identification purposes. A fraudster could trick the user into speaking their name
 5 30 into a microphone 24b, have it validated by the cardholder device and collect the payment credentials from the cardholder device. See Fig. 3b. Similarly, in a simple facial recognition system, where a user's neutral expression 32 is registered on a database, a camera 24c set up by a fraudster could easily catch the user with that neutral expression and thereby have it validated by the
 10 cardholder device and collect the payment credentials from the cardholder device. See Fig. 3c.

There is therefore a need to prevent such fraudulent exploitation of biometric inputs in conjunction with the convenience of mid-range wireless card
 15 technology.

Summary of the Invention

20 According to a first aspect of the invention, there is provided a method of performing a transaction, the method comprising: authenticating a payment account; establishing account holder verification by: detecting a predetermined biometric input from the account holder to establish the presence of the account holder at a point of sale; and detecting an ancillary predetermined user input from the account holder to establish the account holder's consent to the
 25 transaction; and determining whether a payment device associated with the payment account is within a predetermined area, and only requiring detection of an ancillary predetermined user input if the device is not within such a predetermined area.

30 Also disclosed is a method of performing a transaction, the method comprising: authenticating a payment account; and establishing account holder verification by: detecting a predetermined biometric input from the account holder to establish the presence of the account holder at a point of sale; and detecting an ancillary predetermined user input from the account holder to establish the

account holder's consent to the transaction. By including both a (primary) predetermined biometric input and an ancillary predetermined user input, the chances of an account holder inadvertently consenting to a transaction through an accidental (or fraudulently induced) biometric input are reduced.

5

Preferably, detecting the predetermined biometric input comprises one or more of: fingerprint recognition, voice recognition, facial recognition, vein pattern recognition, retinal scanning, and gait analysis.

~~The method may, in some embodiments,~~ As mentioned in the above first aspect,
the method further comprises determining whether a payment device associated
with the payment account is within a predetermined area, and only requiring
detection of an ancillary predetermined user input if the device is not within such
5 a predetermined area. This allows for a user to set defined areas where it is not
required for the ancillary input to be made in order for a transaction to take
place. By way of example, a user can state that they want to be able to consent
to a transaction at a given merchant location only by a single biometric input
(such as a single-digit fingerprint). This may, in some circumstances, be more
10 convenient for the user.

The payment device associated with the payment account may comprise a
secure element in any convenient form factor. Commonly, this would take the
form of a payment card, or an element within a smartphone or other portable
15 computing device, but likewise many other form factors are known and can be
envisaged. Where it is intended for such a payment device to be able to
communicate wirelessly with the terminal, the device would further comprise a
communications interface for establishing that wireless communication.

20 According to a second aspect of the invention, there is provided a transaction
system comprising: a point of sale terminal for processing a transaction; means
for authenticating a payment account; a biometric input device in communication
with the terminal for detecting and verifying a predetermined biometric input
to establish the presence of the account holder; means, in communication with
25 the terminal, for detecting an ancillary predetermined user input from the account
holder to establish the account holder's consent to the transaction; and means
for determining whether a payment device associated with the payment account
is within a predetermined area, and only requiring detection of an ancillary
predetermined user input if the device is not within such a predetermined area.

30 There is further disclosed a transaction system comprising: a point of sale
terminal for processing a transaction; means for authenticating a payment
account; a biometric input device in communication with the terminal for

detecting and verifying a predetermined biometric input to establish the presence of the account holder; and means, in communication with the terminal, for detecting an ancillary predetermined user input from the account holder to establish the account holder's consent to the transaction.

5

The point of sale terminal is typically in communication with a transaction processing and authorising system.

The authenticating means may be configured to detect the presence of an authentic payment account in the payment device.

10