Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

**Datasheet for the decision
of 4 March 2021**

Case Number: T 1746/16 - 3.4.03

Application Number: 12425123.2

Publication Number: 2549421

IPC: G06Q20/00, G07G1/00

Language of the proceedings: EN

Title of invention:
Method and apparatus for the transfer of a money amount by using a two-dimension image code

Applicants:
Cavaterra, Marco
Di Tucci, Cosmo

Headword:

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - (yes) - mixture of technical and non-technical features - skilled person

Decisions cited:

G 0001/19, T 0697/17, T 2314/16, T 1463/11

Catchword:

Case Number: **T 1746/16 - 3.4.03**

D E C I S I O N
of Technical Board of Appeal 3.4.03
of 4 March 2021

Appellant: Cavaterra, Marco
                                  Via del Colle, 3 Lotto 33
(Applicant 1)   00045 Genzano di Roma (RM) (IT)

Appellant: Di Tucci, Cosmo
                                  Strada Colle Montanari 884
(Applicant 2)   04010 Borgo Grappa Latina (IT)

Representative: de Rooij, Mathieu Julien
                                  Bardehle Pagenberg S.L.
                                  Avenida Diagonal 420, 1° 1ª
                                  08037 Barcelona (ES)

Decision under appeal: Decision of the Examining Division of the
                                  European Patent Office posted on 2 March 2016
                                  refusing European patent application No.
                                  12425123.2 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman   T. Häusser
Members: A. Böhm-Pélissier
                     G. Decker

Summary of Facts and Submissions

I.   The appeal is against the decision of the Examining
        Division to refuse European patent application
        No. 12 425 123 on the basis of added subject-matter
        (Article 123(2) EPC) and lack of inventive step
        (Article 56 EPC).

II.   Reference is made to the following documents:
        D1 = US 2008/222048 A1
        D2 = EP 2 128 809 A1
        D6 = EP 1 528 518 A1

III.   During oral proceedings held on 4 March 2021 the
        Appellants filed new claims according to a new Main
        Request. They declared that this request constituted
        their sole request. The Appellants requested that the
        decision under appeal be set aside and a European
        patent be granted in the following version:
        Description: Pages 1 to 12 received during the oral
        proceedings of 4 March 2021;
        Claims: Nos. 1 to 8 of the new Main Request received
        during the oral proceedings of 4 March 2021;
        Drawings: Sheets 1/3 and 3/3 as originally filed and
        sheet 2/3 received during the oral proceedings of
        4 March 2021.

IV.   **Claim 1** of the Main Request reads:

        1. Method for transferring a money amount by using a
        two-dimensional image code (3') between a paying party
        provided with a payment device (42) and a recipient
        party provided with a payment receiving device (41),
        wherein both the paying party and the recipient party

A. Register as a new user at a money transfer managing entity on a server (2), which provides for the management and verification of the paying party and the recipient party and is responsible of the authorization to the transfer of money amounts and their payment; and the method further comprising:

B. Request of the recipient party to the paying party of a money amount, executed between the payment receiving device (41) and the payment device (42);

C. order from the paying party to the money transfer managing entity to pay said money amount to the recipient party, after the insertion of an authorization PIN in the payment device (42) and information communication from the payment device to the server (2);

D. authorization of the payment from the transfer managing entity to the recipient party, with information communication from the server (2) to the payment receiving device (41);

E. payment of said money amount to the recipient party and sending of a confirmation information of effected money amount transfer to the payment device (42) and payment receiving device (41) concerning the effected payment of the money amount, or possible writing off or cancellation of an already effected payment operation; the method being characterized in that said payment device (42) is a payment mobile phone and said payment receiving device (41) is a payment receiving mobile phone, and in that:

a mobile phone software module is installed on both the payment mobile phone and the payment receiving mobile phone,

- in step B, the recipient party generates through the mobile phone software module installed on the payment receiving mobile phone a two-dimensional image code (3') containing the money amount, a USER-ID of the

recipient party from a personal details archive (14) on the payment receiving mobile phone and further containing information characterizing the transaction retrieved from an operations archive (16) in the payment receiving mobile phone and visualizes the two-dimensional image code on the display of the payment receiving mobile phone;
- in step B, the payment mobile phone of the paying party captures the two-dimensional image code (3') from the display of the recipient party mobile phone;
- in step C, the mobile phone software module on the payment mobile phone analyzes the two-dimensional image code and the payment mobile phone sends to the server (2) of the money transfer managing entity an encrypted authorization SMS message, the encrypted authorization SMS message including data contained in the two-dimensional image code (3'), comprising the indication of said money amount,
- in step D, the server (2) receives said encrypted authorization SMS message and authorizes or not the payment of the money amount,
- the payment receiving mobile phone of the recipient party restricting itself in step B to the generation and visualization of said two-dimensional image code (3'), without sending any relevant information to the server of the money transfer managing entity, wherein the two-dimensional image code (3') presented by the payment receiving mobile phone and captured by the payment mobile phone, provides as guarantee of the privacy only the user-ID of the recipient party, an operation number, the money amount, the phone number of the payment receiving mobile phone and wherein, the payment mobile phone visualizes on the display the transaction money amount and requests the typing of the authorization PIN, extracts from a "personal details" archive the user-ID of the paying party, extracts from

a "keys" archive the encryption key for the
authorization PIN, encrypts the authorization PIN,
composes an authorization SMS message and sends the
authorization SMS message to the server (2).

Reasons for the Decision

1.   **The invention as claimed**

1.1   The invention concerns a payment method via mobile
          phone. The objective is that sensitive data does not
          need to be sent from the merchant's device to the
          server, to eliminate expensive and dedicated Point Of
          Sale (POS) devices (devices used by the merchant at the
          checkout) and to unload the network.

1.2   The invention proposes using two mobile phones. The
          merchant's mobile phone transfers all data relevant for
          the payment transaction via QR code to the customer's
          mobile phone. The payment data is then transmitted from
          the customer's mobile phone to the server via encrypted
          SMS including the authorisation PIN.

1.3   The method has the advantage that for the transaction
          only one single SMS message has to be sent via the
          mobile phone network. The customer can also play the
          role of the merchant by using the same software
          application. The personal information of the customer
          does not need to be given to the merchant during the
          transaction.

2.   **Main Request**

2.1   **Technicality**

All the features of claim 1 are implemented on a mobile
phone and are therefore technical. Some features, when
not executed on the mobile phone, are related to a
business method. Therefore they may be included into
the formulation of the problem.

2.2   **Closest prior art**

Closest prior art is document D1, because it has the
most features in common and relates to a similar
payment method using a mobile phone and bar codes.

2.3   **D1**

2.3.1   D1 discloses a payment method, where the payment device
is a mobile phone and the payment receiving device is a
point-of-sale (POS) device. The objective in D1 is to
avoid the installation of specific software and
sensitive codes on the mobile device. Therefore
communication "route A" (see amended Fig. 1 below) is
chosen. D1 discloses encrypting information in one-
dimensional bar codes. D1 teaches in the context of the
discussion of the prior art the use of encoding
information in mobile phones by using (two-dimensional)
QR codes.

2.3.2   In D1 the transaction needs at least five
communications via the Intranet (see figure below):
(1) payment data is transmitted from the merchant's
    device to a server via Internet;
(2) a bar code is transmitted to the merchant's device
    and shown to the client's mobile phone;

>   (3) the bar code received by the client is forwarded to
>   the server, decoded and verified there;
>   (4) the server then requests via the network a PIN code
>   for finally authorising the financial transaction;
>   (5) the client transmits the PIN to the server.
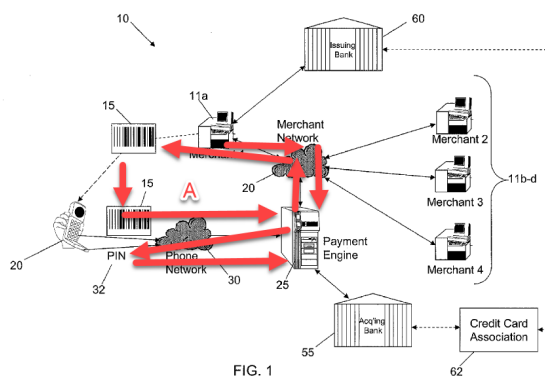
FIG. 1

*D1, Fig. 1; bold arrows ("route A") added by the
Board for illustrating the routes of communication
during the financial transaction.*

2.4   Difference

2.4.1   The preamble of claim 1 is disclosed in D1 in
paragraphs [0018] to [0040] and in Figs. 1 to 4. In
particular, registering of the parties is disclosed in
paragraphs [0021] and [0022] and Fig. 4.

2.4.2   D1 fails to disclose (using the claim wording of
claim 1, but referring to D1; the distinguishing
features not disclosed in D1 are highlighted using
underlining by the Board)
(A) that said payment receiving device (11a) is a
payment receiving mobile phone;
(B) a [*i. e. the same*] mobile phone software module is
installed on both the payment mobile phone and the
payment receiving mobile phone (*referring back to "the"
software module further below in the claim for both the
payment mobile phone and the payment receiving mobile*

*phone implies that the same software module is
installed on both devices*),

(C)- in step B, the recipient party generates <u>through
the mobile phone software module installed on the
payment receiving mobile phone device a two-dimensional</u>
image code (*D1 only discloses a one-dimensional bar
code generated by the server and transmitted via the
POS device*)

(D) containing the money amount, a USER-ID of the
recipient party <u>from a personal details archive</u> (*D1
fails to disclose such an archive*) <u>on the payment
receiving mobile phone</u>

(E) and further containing information characterizing
the transaction <u>retrieved from an operations archive</u>
(*D1 fails to disclose such an archive*) <u>in the payment
receiving mobile phone</u> and visualizes the <u>two-
dimensional</u> image code on the display <u>of the payment
receiving mobile phone</u>; - in step B, the payment mobile
phone of the paying party captures the two-dimensional
image code from the display <u>of the recipient party
mobile phone</u>;

(F) in step C, <u>the mobile phone software module on the
payment mobile phone analyses the two-dimensional image
code</u> (*in D1, paragraph [0036], it is mentioned that
only decoding the UPC code may take place in the mobile
phone; interpretation, i. e. decoding and analysing the
encoded information, is however always performed in the
server 25, see paragraph [0039] and Fig. 3 of D1*)

(G) and the payment mobile phone sends to the server of
the money transfer managing entity an <u>encrypted
authorization SMS message</u> (*D1 does not mention an
encryption of the SMS in the general sense of
understanding encrypting SMS messages with an
encryption key; D1 discloses in paragraph [0036] that
either the bar code image or the decoded UPC code is
sent via an unsecured network*), the <u>encrypted</u>

authorization SMS message including data contained in the two-dimensional image code, comprising the indication of said money amount, - in step D, the server (25) receives said encrypted authorization SMS message and authorizes or not the payment of the money amount,

(H) - the payment receiving mobile phone of the recipient party restricting itself in step B to the generation and visualization of said two-dimensional image code (*in D1 the recipient party sends all relevant data to the server 25 requesting the generation of a bar code, see paragraphs [0034] and [0035]*),

(I) without sending any relevant information to the server of the money transfer managing entity (*the server 25 receives inter alia the amount and encodes it into the bar code sent back to the merchant*), wherein

(J) the two-dimensional image code presented by the payment receiving mobile phone and captured by the payment mobile phone, provides as guarantee of the privacy only the user-ID of the recipient party, an operation number, the money amount, the phone number of the payment receiving mobile phone (*in D1, paragraph [0035], not the phone number, but other parameters such as the currency and VAT tax being charged are mentioned*) and wherein,

(K) the payment mobile phone visualizes on the display the transaction money amount (*in D1 the amount cannot be decoded and displayed in the customer's mobile phone*) and requests the typing of the authorization PIN (*in D1 the PIN is requested by the server*),

(L) extracts from a "personal details" archive the user-ID of the paying party (*D1 discloses neither a "personal details" nor a "keys" archive*),

(M) extracts from a "keys" archive the encryption key for the authorization PIN (*in D1 encryption takes place*

in the "Encryption Component 48" on the server 25, see
paragraph [0032] and Fig. 2),
(N) <u>encrypts the authorization PIN</u> (*in D1 the server*
sends a separate request for the PIN, see paragraph
[0040]),
(O) <u>composes an authorization SMS message</u> (*the SMS*
message sent in D1 cannot be considered to be an
authorization message, since authorization takes place
in a separate step via entering the PIN into the
request form sent by the server to the customer or via
a voice call, see paragraph [0040]) and sends the
<u>authorization SMS message</u> to the server.

2.5   Effects

In accordance with the submissions of the Appellants in
section I.3.2 of the letter dated 12 January 2016 and
the discussions during the oral proceedings before the
Board, the technical effects of these fifteen differing
features can be summarised as follows:
(a) obviating the need for an expensive and dedicated
    POS device and the relevant connections with the
    server (Feature (A)),
(b) providing an efficient way of transferring
    information from the merchant to the buyer
    (Features (C), (D), (E), (F), (G), (H), and (J));
(c) the same device (mobile phone) being able to carry
    out both the function of buying and the function of
    selling depending on the need and according to a
    precise sequence of steps (Features (B), (C), (D),
    (E), and (F));
(d) the complete control of the financial transaction
    being within the paying party, thus guaranteeing
    the privacy of the paying party (Features (H), (I),
    (J), (K), (L), (M), (N), and (O));

(e) unloading the server, reducing the number of
    communications to a minimum and allowing a faster
    transaction while maintaining a high security level
    (Features (C), (D), (E), (F), (G), (H), (I), (J),
    (K), (L), (M), (N), and (O));

(f) making the transaction independent from any network
    other than the mobile phone network (Features (H),
    (I), (J), (K), (M), (N), and (O));

(g) the software providing full control of the
    transaction by analysing/displaying the data (of
    the two-dimensional image code), displaying the
    amount, providing archives for keys, PINs, IDs, and
    encrypting them (Features (B), (C), (D), (E), (F),
    (G), (J), (K), (L), (M), and (N)).

2.6   **Problem**

Since Feature (A) on the one hand and Features (B) to
(O) on the other hand are not functionally
interdependent, it is appropriate to formulate partial
problems in relation to these sets of features. The
problem can therefore be formulated as achieving effect
(a) (first partial problem) as well as effects (b) to
(g) (second partial problem).

2.7   **Non-Obviousness**

(A) First partial problem (effect (a))

2.7.1 Obviating the need for an expensive and dedicated POS
       device is solved by replacing the POS by a mobile
       phone. Even though the replacement of a POS is not
       directly motivated by the teaching of document D1, the
       skilled person would, when attempting to achieve the
       technical effect (a), consider the prior art documents
   discussed in document D1 and in particular the

disclosure of document D6 (paragraphs [0023] and
[0025]). They would thus be led in the Board's judgment
to the solution claimed in Feature (A).

(B) Second partial problem (effects (b) to (g))

2.7.2   The Appellants have argued that whether or not the bar
         code is generated by a merchant mobile phone or is
         generated remotely and sent to a mobile phone did not
         affect a customer experience in any way, and applying
         the reasoning of e. g. T 2314/16 and T 1463/11
         (specifically Reasons 11 to 17) cannot be regarded as
         part of business considerations of the notional
         business person.

2.7.3   The Board is of the opinion that using two-dimensional
         image codes is a well-known alternative to one-
         dimensional bar codes for the skilled person in the
         relevant technical field of software engineering. This
         includes generating and decoding bar codes on a mobile
         phone. Using a two-dimensional code is furthermore
         suggested by the prior art discussed in the present
         description in paragraphs [0004] and [0005], in the
         prior art discussed in D1 (paragraph [0005]) and in
         document D2 (paragraph [0057]).

2.7.4   However, using one and the same type of device (mobile
         phone) and corresponding software for carrying out both
         the function of buying and the function of selling
         depending on the need and according to a precise
         sequence of steps is not suggested in any of the
         documents cited above. Starting from D1 and complying
         with the concept that the server controls the
         transaction and matches both the merchant's and
         customer's action - while maintaining a high security
         level -, one and the same software on the mobile

devices would be counter-productive. If the skilled
person replaced the POS device of document D1 by a
mobile phone, they would consider a specific
corresponding software tailored to the need of the
seller in order to guarantee the required safety level.
D1 explicitly teaches to reduce any software to be
installed (paragraphs [0008], [0009] and [0018]). In
view of the teaching of D1 the skilled person would
therefore reduce these modules to a minimum. This
teaches away from a more complex universal solution.

2.7.5   Moreover, in order to achieve the technical effects (d)
        and (e) starting from D1, the skilled person would have
        to implement "route B" for reducing the number of
        communications:
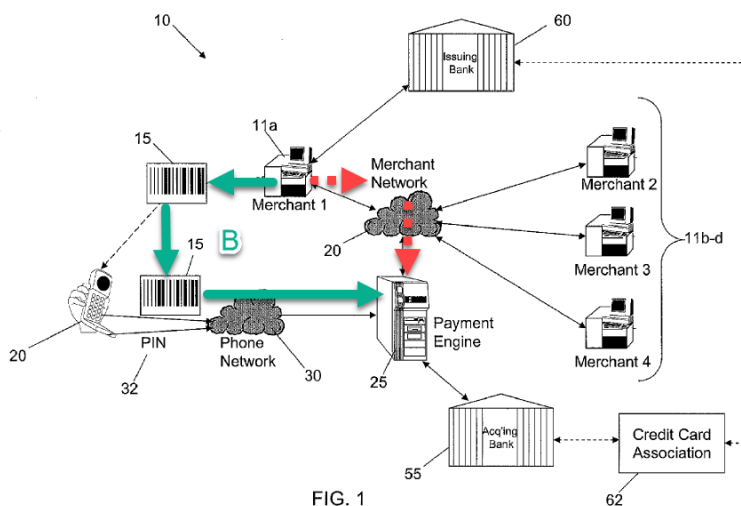
FIG. 1

*D1, Fig. 1, solid arrows ("route B") added by the
Board; dotted arrows illustrate matching of merchant's
data with the customer's data on the server.*

2.7.6   This "route B" however is against the teaching and
        objective of D1, i. e. avoiding software to be
        installed on the mobile phone and avoiding sensitive
        information like PIN codes or encryption keys being
        installed on the mobile phone.

2.7.7   "Route B" would first require that the merchant create
        the two-dimensional image code on their mobile phone.
        This however would be contrary to the concept of D1,
        where the server controls the transaction. The prior
        art also teaches away from encoding sensitive
        information, such as the authorisation PIN code, into
        the authorisation SMS message sent to the server:

2.7.8   The skilled person would always seek for a balance
        between security requirements and unloading the
        network. In view of the teaching of D1, where security
        has first priority, the skilled person would not
        abandon a separate PIN request. Given the teachings of
        D1 and D2 (see abstracts) the skilled person would not
        abandon the matching of merchant's and customer's data
        by the server, either. Therefore, a communication
        between the merchant's device and the server is always
        required in addition to the communication from the
        customer to the server. None of the documents cited
        above provides any teaching that the transaction is at
        the same time (1) reduced to one single communication,
        i. e. the authorisation SMS of the paying party, (2)
        performed without any message between merchant and
        server for matching the merchant's and client's
        request, and (3) performed without a separate
        authorisation PIN request.

2.7.9   The approach proposed by the invention has the
        advantage that only one request has to be transmitted
        via the mobile phone network without connection to the
        Internet or a similar network. This makes the method
        independent from any wired structure and insensitive to
        network interruptions during the transaction or between
        two transaction transmissions. These interruptions
        would lead to an insecure situation. The proposed
        solution is both save and unloads the network by

providing only one single communication via the mobile
phone network. It considerably reduces data traffic.
During shopping events like "Black Friday" or the days
prior to Christmas, where there can be thousands or
millions of payments being made at the same time, the
invention offers the benefit that for each of these
transactions only one single data transmission to the
server is needed, instead of five or more.

2.7.10 This is realised by decoding and analysing in the
        customer's mobile phone the two-dimensional image code
        comprising the transaction data (IDs of merchant and
        customer, transaction amount, transaction code, phone
        numbers). The data is encrypted with an encryption key
        into an encrypted SMS message comprising in addition
        the authorisation PIN.

2.7.11 If - starting from document D1 - the skilled person
        considered to replace the POS device by a mobile phone,
        there would still be a communication between the
        merchant's device and the server (via the mobile phone
        network) for matching the data and in total at least
        one communication in addition to the communication
        between the customer and the server, thus leading to
        different subject-matter than defined in the claims.

2.7.12 Document D1 only teaches to decode the UPC code of the
        one-dimensional bar code in the buyer's mobile phone
        without analysing the content, i. e. linking the
        transaction information to the UPC code. This can only
        be done on the server where the corresponding data is
        saved. The solution of D1, where the transaction is
        controlled by the server, therefore teaches away from
        the present solution which proposes to save the
        authorisation PIN for the server on the customer's
        mobile phone together with all the other transaction

information in order to reduce the number of
transaction communications.

2.7.13   The prior art cited above is completely silent about
         Features (H) to (M), i. e. the details of the software
         implementation of the transaction method, handling the
         data, decoding and encryption. These features
         contribute to realising a transaction method which
         effectively unloads the network while maintaining a
         high security standard and high safety level for the
         transaction. Therefore, these features contribute to
         the technical effect of the invention, though some of
         them may be considered as non-technical features (see
         G 1/19, point 85 and T 0697/17, point 5.2.5).

2.7.14   In summary, nothing in the prior art would lead the
         skilled person to the combination of all the features
         of claim 1. The subject-matter of claim 1 is therefore
         inventive.

2.7.15   Independent system claim 8 corresponds essentially to
         method claim 1. Claims 2 to 7 are dependent on claim 1.

2.7.16   Accordingly, the subject-matter of claims 1 to 8
         involves an inventive step (Articles 52(1) and 56 EPC).

3.   **Conclusion**

         For the above reasons the board is of the opinion that
         the application and the invention to which it relates,
         in the version according to the appellant's sole
         request, meet the requirements of the EPC. Hence, a
         patent is to be granted on the basis of that version
         (Articles 97(1) and 111(1) EPC).

Order

For these reasons it is decided that:

1.   The decision under appeal is set aside.

2.   The case is remitted to the examining division with
        the order to grant a patent in the following version:

   Description: Pages 1 to 12 received during the oral
   proceedings of 4 March 2021;

   Claims: Nos. 1 to 8 of the new "Main Request" received
   during the oral proceedings of 4 March 2021;

   Drawings: Sheets 1/3 and 3/3 as originally filed and
   sheet 2/3 received during the oral proceedings of
   4 March 2021.

The Registrar: The Chairman:

S. Sánchez Chiquero   T. Häusser

Decision electronically authenticated