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

Datasheet for the decision of 13 November 2014

Case Number: T 1072/09 - 3.5.01

Application Number: 00960021.4

Publication Number: 1218837

IPC: G06F17/60

Language of the proceedings: EN

Title of invention:
METHOD OF AND SYSTEM FOR MAKING PURCHASES OVER A COMPUTER NETWORK

Applicant:
MasterCard International Incorporated

Headword:
Online payment/MASTERCARD

Relevant legal provisions:
EPC 1973 Art. 56, 84
RPBA Art. 8(3)

Keyword:
Inventive step - (no)

Decisions cited:
T 0641/00, T 1784/06

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 1072/09 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 13 November 2014

Appellant: (Applicant)	MasterCard International Incorporated 2000 Purchase Street Purchase, NY 10577 (US)
Representative:	Holme, Edvard Holme Patent A/S Valbygårdsvej 33 2500 Valby (DK)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 23 December 2008 refusing European patent application No. 00960021.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	S. Wibergh
Members:	K. Bumes
	P. Schmitz

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse European patent application No. 00960021.4, *"Method of and system for making purchases over a computer network"*, published as

A1: WO-A1-01/18719,

for lack of inventive step (Article 56 EPC 1973) over

D1: EP-A-0 921 487, *"Method and system for billing on the internet"*.

II. In the statement setting out the grounds of appeal, the appellant requested that the decision of the examining division be set aside and that a patent be granted on the basis of a main request or a first or second auxiliary request, all requests filed with the statement of grounds.

The arguments in the statement setting out the grounds of appeal can be summarised as follows:

(a) Since D1 uses a prepaid card and not an ATM card, it is intended for a completely different purpose.

(b) In D1, the terminal does not send the password over the Internet but will instead send the result of an operation performed on the password.

(c) The operation on the password uses a protocol (CHAP, Challenge Handshake Authentication Protocol) which is different from the encryption in the present application.

(d) In the present application, the PIN is not known to the third party contractor beforehand, which proves a higher level of security.

(e) Since the first and second numbers in D1 do not contain personal or confidential data, it would not make sense to use encryption.

III. The Board appointed oral proceedings, as requested on an auxiliary basis, and annexed a preliminary opinion to the summons. The Board expressed the view that the claims seemed to refer to a business method set up on a generic computer infrastructure. Authorising an account holder by means of a PIN and securing a payment from the account holder to a second party by means of encryption and a trusted third party appeared to be well-known.

IV. In response to the summons, the appellant filed another auxiliary request, to be inserted as the first auxiliary request, and renumbered the two previous auxiliary requests accordingly. A complete set of all requests was filed (10 October 2014).

(a) Claim 1 according to the main request reads:

"1. A method of making a purchase to be made over a computer network (24) using a first number that identifies a consumer's account from which funds will be withdrawn to pay a purchase price and a second number associated with said first number which, when used with said first number, enables withdrawal of funds from said account, said method comprising the steps:

- transmitting said first number over said network (24) from a consumer location (14) to an on-line merchant location (18);
- forwarding said first number over said network (24) from said on-line merchant location (18) to a third party contractor location (22);
- transmitting a query for said second number over said network (24) from said third party contractor location (22) to said consumer location (14);

- transmitting said second number over said network (24) from said consumer location (14) to said third party contractor location (22); bypassing said on—line merchant location (18); and
- after receiving said first number and said second number at said third party contractor location (22), verifying the validity of said first number and said second number at said third party contractor location (22),
- wherein said first number and said second number are transmitted via encrypted connections."

(b) The first auxiliary request appends the following paragraphs to claim 1 of the main request:

"- said method further including the step of transmitting a signal over said network (24) from said third party contractor location (22) to said on—line merchant location (18) indicating whether said first number and said second number are valid, and
- the additional step of transmitting a signal over said network (24) from said on—line merchant location (18) to said consumer location (14) indicating whether said purchase has been authorized."

(c) As compared to claim 1 of the main request, the second auxiliary request omits two paragraphs (relating to a query from the third party location and to encrypted connections, respectively) and appends the following paragraph to claim 1:

"- wherein said first number and said second number are simultaneously transmitted to said third party contractor location (22)."

(d) As compared to claim 1 of the main request, the third auxiliary request replaces the last paragraph (relating to encrypted connections) with the following paragraph:

"- wherein said first number is an ATM card number and said second number is a PIN associated with said ATM card number."

V. In the written response to the summons, the appellant presented the following additional arguments in favour of an inventive step.

The first and second numbers were transmitted to a third contractor location along different routes to ensure that the consumer's payment data could not be used even if one of the numbers was intercepted. Security was further enhanced by sending the numbers over encrypted connections.

On-line verification of an account number was not known at the priority date of the present application. In 1999, only a single number (card number) was used for on-line purchases. On-line merchants were not able to verify PINs.

The first auxiliary request addressed the additional problem that both the merchant and the consumer wanted to know whether a purchase could be completed. The third party contractor provided feedback on a payment authorisation to the on-line merchant who in turn informed the consumer.

Accordingly, the method of claim 1 (all requests) was considered to be new and non-obvious over the available prior art, in particular D1.

VI. At the oral proceedings before the Board, the prior art discussion focused on document D1. The appellant pointed out that D1 aimed at an Internet billing method which could be used without a credit card (paragraph 0005): D1 proposed prepaid cards for specific purposes (paragraphs 0023 and 0050). As the ID number of a dedicated prepaid card required less secrecy than the number of a general purpose credit card, the authentication process of D1 (paragraphs 0039/0041; Figure 1, S102; Figure 4, 201; Figure 5, S204) did not encrypt the card number, and there was no obvious reason for encrypting it.

Claim 1 according to the first auxiliary request ensured that the on-line transaction could be completed by notifying the merchant and the consumer whether the payment had been authorised.

Regarding the simultaneous transmission specified by claim 1 of the second auxiliary request, the appellant argued that this feature (not deriving from Figure 2 of the application) reflected language of the description (page 3, line 20; page 9, line 20) and was supported by computer programs annexed to the description. Simultaneous transmission of the first and second numbers allowed faster authorisation processing and was not envisaged or suggested by D1.

The third auxiliary request clarified that the payment card was a general purpose card which could be used spontaneously at different locations. As the prepaid card of D1 presupposed a pre-existing business relationship between the card holder and a specific on-line merchant, it was not obvious to use the payment procedure of D1 for general payment cards. By-passing

the merchant in the verification process provided a simple solution to a serious problem.

The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main request or any one of auxiliary requests 1 to 3 filed with letter dated 10 October 2014.

Reasons for the Decision

1. The application aims at a secure scheme for making payments over a non-secure computer network. The scheme verifies a consumer's account number (e.g. ATM card number) with the help of an associated personal identification number (PIN). The consumer supplies his account number to an on-line merchant while supplying the PIN to a third party (bank) and never to the merchant (A1, page 2, lines 10 to 22; page 8, lines 21 to 24; page 11, 4/5). The third party receives both numbers which may have been transmitted "simultaneously" to it from the merchant computer and the consumer computer, respectively (page 8, lines 18 to 21). The third party verifies the correctness of the numbers (by accessing an internal database or contacting the card issuing bank), checks for sufficiency of funds, and either authorises or denies the transaction; the authorisation or denial is communicated to the on-line merchant, who either completes or rejects the purchase and so notifies the consumer (A1, page 3, lines 5 to 13; page 10, lines 18 to 23; Figure 2). The numbers are preferably transmitted via encrypted connections (A1, page 7, lines 18 to 20; page 8, lines 4/5 and 21/22; original claims 3 and 11).

Main request

Article 56 EPC 1973 - Inventive step

2. In the light of Article 52(1)(2)(3) EPC, Article 56 EPC 1973 requires a non-obvious technical contribution (see e.g. T 641/00-*Two identities/COMVIK*, Headnote 1, OJ EPO 2003, 352; T 1784/06-*Classification method/COMPTEL*).

3. While claim 1 refers to a method of making a "purchase" over a computer network, the method focuses on a payment scheme. In either case, document D1 --- "*Method and system for billing on the Internet*" --- represents the closest available prior art.

D1 (e.g. Figure 1) describes its on-line billing method in relation to a prepaid card (paragraphs 0001, 0023). A consumer (terminal 100) sends a request to an on-line merchant (content server 200) for some content or service. The request message may include a first number, namely an ID of the card to be used for the payment (paragraph 0039; Figure 3). The merchant sends an authentication and billing request to a card management server (300) acting as a third party; that request may forward the card ID (paragraphs 0039, 0041). After receiving the authentication and billing request, the card management server requests password information from the consumer terminal. The consumer terminal generates that information by concatenating the password (i.e. a second number, PIN, associated with the card) with a random number (challenge) provided in the request from the card management server (paragraphs 0028, 0041). The result of that mathematical operation is transmitted to the card management server. The card management server performs

the same operation on a password stored in relation to the card ID, and compares its result with the reply received from the consumer terminal. If they match, the authentication succeeds.

In other words, the consumer terminal according to D1 does not send a clear version of the password to the card management server but effectively encrypts the password for transmission to the third party.

4. D1 is silent on how the consumer terminal (100) sends the card ID to the merchant (200) (D1, column 15, lines 7 to 12) and on how the merchant (200) forwards the card ID to the card management server (300) (paragraph 0041).

Therefore, the method of claim 1 differs from D1 (only) in that the first number (card ID) is explicitly said to be transmitted via encrypted connections (from the consumer to the merchant and from the merchant to the third party).

5. However, using an encrypted Secure Socket Layer (SSL) is a conventional way of safely transmitting data packets according to the Internet protocol, as acknowledged in the present application (A1, page 2, lines 2 to 4: "most popular approach"). Notably banking schemes use that layer or any other security protocol (https). When such a secure transport layer is used, it is used for the whole data traffic under that protocol; no selective exception is made for data items that might be less sensitive among the bulk of data being transmitted.

Hence, it is obvious to transmit also the first number (card ID) via the encrypted connections typically used for data streams including sensitive items.

6. Therefore, the Board does not identify any non-obvious technical contribution in the method according to claim 1 of the main request.

First Auxiliary Request

7. According to claim 1 of the first auxiliary request, the third party informs the merchant whether the first and second numbers have been verified as valid, and the merchant informs the consumer accordingly.

8. The merchant and the consumer obviously want to know whether the requested purchase can be carried out, *i.e.* whether the payment has been authorised by the third party. Accordingly, the card management server of D1 notifies the content server of the authentication result (D1, Figure 1, step S104), and the card management server notifies the consumer terminal of the remaining balance (D1, Figure 5, step S211). The merchant's content server starts providing the requested service to the consumer terminal and, thus, effectively informs the consumer that the authentication was successful.

9. Hence, the first auxiliary request does not add any non-obvious step to the purchasing method.

Second Auxiliary Request

10. According to claim 1 of the second auxiliary request, the first number (account number) and the second number

(PIN) are "simultaneously" transmitted to the third party.

That feature needs to be construed in the light of the description which is supposed to support the claim (Article 84 EPC 1973). The only comprehensible basis for a simultaneous action is provided on pages 7 and 8 of the present application.

Page 7, last paragraph:
"When the on-line merchant receives the ATM card number, or earlier, the second computer 16 creates a unique session identifier [...] The ATM card number is then forwarded, or echoed, over the Internet by the second computer 16 to the third computer 20 at the third party contractor location 22 [...]"

Page 8, lines 18 to 21:
"Simultaneously or soon thereafter, the second computer executes a hyperlink to the third computer and the consumer is prompted by the third computer to input his PIN (block 42). The consumer inputs his PIN into the first computer 12 and transmits it over the Internet to the third computer 20 (block 44)."

The program code lists annexed to the description of the present application do not bring out any other concept of simultaneity and, thus, do not justify any other construction of claim 1.

11. The type of simultaneous action described by the present application --- the third party receives an account number and then prompts the consumer to provide an associated PIN/password --- is already used in the method of D1 (see Figure 1, steps S012, S103; Figure 8, steps S501, S502).

12. Hence, the second auxiliary request does not add any non-obvious step to the payment method.

Third Auxiliary Request

13. According to claim 1 of the third auxiliary request, the first number is an ATM card number and the second number is a PIN associated with the ATM card number.

14. The Board first notes that the technical character of defining an account number as an ATM card number is questionable. The Board also points out that D1 aims at an Internet billing method which "*can be*" used without a credit card (D1, paragraph 0005). However, that wording suggests that the method of D1 may in principle continue using a credit card if the inherent risk is accepted by the users (which is not a technical choice). Objectively, the method of D1 lends itself to all types of cards using a password (or PIN) to authenticate its owner.

The concept of D1 tying a card number to a password matches the concept of the present application (see A1, page 7, lines 16 to 18): "As used herein, the term "ATM card" includes bank cards, debit cards and any other cards for which the issuing bank or organization may require a valid PIN for use."

15. The appellant argued that the present application provided a simple solution to a serious, long-standing problem and, therefore, the solution should be acknowledged as inventive.

However, the solution is almost anticipated by the method of D1. In particular, the central problem that on-line merchants need security about the authenticity of a card user is addressed and solved by D1 in that the card user is required to provide a password (or PIN) without giving the confidential password away to the merchant.

16. On the technical implementation level, transmitting data among networked computers, prompting participants for data input, and encrypting sensitive data do not entail any non-obvious consideration. The cognitive meaning of the transmitted data does not have any non-obvious implication for the technical functioning of the servers or clients or their interconnecting network.

17. Hence, the third auxiliary request does not add any non-obvious aspect to the payment method.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: On behalf of the Chairman
(according to Art. 8(3) RPBA):

T. Buschek K. Bumes

Decision electronically authenticated