(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 May 2010 (14.05.2010)

PCT

(10) International Publication Number
WO 2010/053899 A4

(51) International Patent Classification:
G06Q 20/00 (2006.01) *G06F 21/00* (2006.01)

(21) International Application Number:
PCT/US2009/063067

(22) International Filing Date:
3 November 2009 (03.11.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/112,124 6 November 2008 (06.11.2008) US

(71) Applicant *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128-8999 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WELLER, Kevin** [US/US]; 63 Fernwood Drive, San Anselmo, California 94960 (US). **STEELE, Kim** [US/US]; 24129 Heather Hill Place, Aldie, Virginia 20105 (US). **KOGANTI, Krishna Prasad** [US/US]; 7985 Pumpkin Court, Cupertino, California 95014 (US). **FAITH, Patrick** [US/US]; 2810 Jones Gate Court, Pleasanton, California 94566 (US).

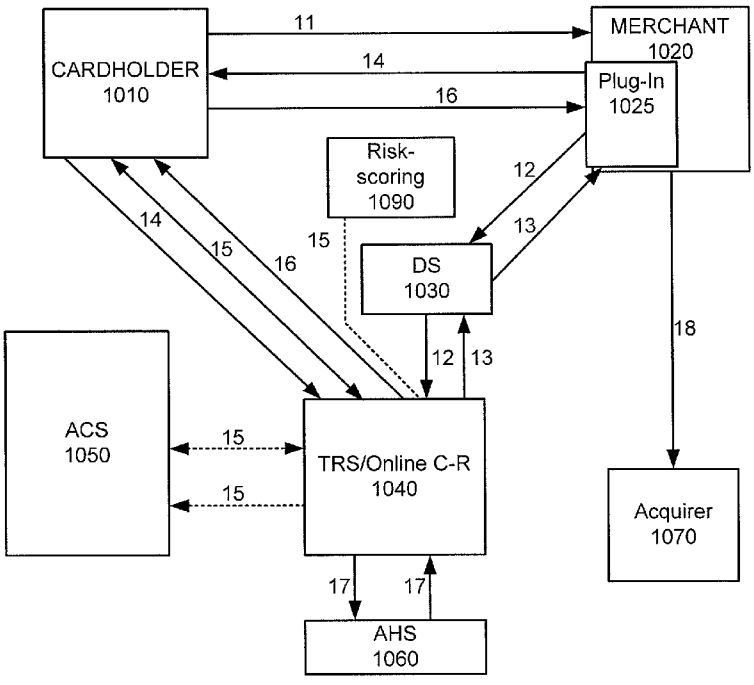
(74) Agents: **JEWIK, Patrick R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: ONLINE CHALLENGE-RESPONSE



(57) Abstract: Embodiments of the invention enable cardholders conducting an online transaction to be authenticated in real-time using a challenge-response application. The challenge-response application can be administered by an issuer or by a third party on-behalf-of an issuer. A challenge question can be presented to the cardholder, and the cardholder's response can be verified. The challenge question presented can be selected based on an analysis of the risk of the transaction and potentially other factors. A variety of dynamic challenge questions can be used without the need for the cardholder to enroll into the program. Additionally, there are many flexible implementation options of the challenge-response application that can be adjusted based on factors such as the location of the merchant or the location of the consumer.

WO 2010/053899 A4

WO 2010/053899 A4

Published:

— *with international search report (Art. 21(3))*

— *with amended claims and statement (Art. 19(1))*

(88) Date of publication of the international search report: 12 August 2010

Date of publication of the amended claims and statement: 23 September 2010

AMENDED CLAIMS
received by the International Bureau on 15 July 2010 (15.07.2010)

1. A system for authenticating a consumer conducting a transaction, the system comprising:

a challenge-response server computer, the challenge response server computer comprising modules capable of executing on the challenge-response server, the modules comprising:

a risk analyzer module configured to obtain a risk score for the transaction; and

a challenge optimizer module configured to generate an authentication challenge using the risk score, and configured to compare a response received from the consumer to an expected response, wherein the challenge-response server computer is configured to receive an enrollment request message and is configured to send an enrollment response message.

2. The system of claim 1 further comprising:

a password-based authentication system, wherein the password-based authentication system is configured to provide a password-based authentication of the consumer conducting the transaction.

3. The system of claim 2 wherein the password-based authentication system is configured to provide authentication of the consumer substantially concurrently to the authentication provided by the challenge-response server.

4. The system of claim 2 wherein parameters of the authentication provided by the challenge-response server and parameters of the authentication provided by the password-based authentication system are determined based on information about the transaction being conducted and on information on the account being used to conduct the transaction.

5. The system of claim 2 wherein the authentication provided by the challenge-response server is provided when the password-based authentication of the consumer cannot take place.

6. The system of claim 1 wherein challenge-response server is configured to authenticate the consumer substantially concurrently with an enrollment process for the password-based authentication system that occurs during the transaction; and wherein the challenge-response server computer is configured to calculate the risk score.

7. The system of claim 1 wherein challenge-response server authenticates the consumer substantially concurrently with a password recovery process for the password-based authentication system that occurs during the transaction.

8. The system of claim 1 wherein the challenge-response server computer comprises a device information module configured to obtain information on a device used by the consumer to conduct the transaction.

9. A computer implemented method of authenticating a consumer conducting a transaction with a merchant, the method comprising:

a) receiving a request for consumer authentication at a server computer, the request including information about the transaction being conducted and information on an account being used to conduct the transaction, wherein the server computer sends an authentication message to the merchant if the account can be authenticated;

b) determining a risk score for the transaction at the server computer;

c) if the account can be authenticated, sending an authentication challenge to the consumer when the risk score exceeds a threshold, the authentication challenge comprising a question whose response is static, dynamic or semi-dynamic;

d) receiving a consumer response to the authentication challenge;

e) comparing the consumer response to an expected response; and

f) authenticating the consumer conducting the transaction when the expected response and the consumer response are substantially the same.

10. The method of claim 9 wherein a)-f) are performed substantially concurrently with a password-based authentication of the consumer conducting the transaction.

11. The method of claim 10 wherein a)-f) are performed when the risk score is a medium risk score, and wherein no challenge is sent if the risk score is a low risk score and a transaction failure message is sent if the risk score is a high risk score.

12. The method of claim 9 wherein a)-f) are performed when a password-based authentication of the consumer conducting the transaction cannot take place.

13. The method of claim 9 wherein a)-f) are performed substantially concurrently with an enrollment process for a password-based authentication of the consumer conducting the transaction.

14. The method of claim 9 wherein a)-f) are performed substantially concurrently with a password recovery process for a password-based authentication of the consumer conducting the transaction.

15. The method of claim 9 wherein a)-f) are performed instead of a password recovery process for a password-based authentication of the consumer conducting the transaction.

16. The method of claim 9 further comprising:

sending the expected response to a consumer device,

wherein the expected response sent to the consumer device is valid for only one transaction.

17. The method of claim 9 wherein the risk score is further based on querying an external risk assessment system.

18. The method of claim 9 wherein the authentication challenge is generated by a payment processing network.

19. The method of claim 9 further comprising:

sending the risk score to a server computer associated with an issuer of the account being used to conduct the transaction;

wherein the authentication challenge is generated by the server computer associated with the issuer and wherein the consumer response is received by the issuer.

20. A computer-readable medium comprising computer-executable code, executable by a processor, for performing the method of claim 9.

21. A server computer comprising a processor and the computer readable medium of claim 20 coupled to the processor.

STATEMENT UNDER ARTICLE 19

The claims in the substitute pages differ from those originally filed by amending claims 1 and 9.

In claim 1, the phrase "wherein the challenge-response server computer is configured to receive an enrollment request message and is configured to send an enrollment response message" was added.

In claim 9, the phrase ", wherein the server computer sends an authentication message to the merchant if the account can be authenticated" was added to a) and "if the account can be authenticated" was added to c).

In view of the foregoing, Applicants believe all claims now pending in this Application are novel.

Respectfully submitted,

/David B. Raczkowski/

David B. Raczkowski