US Patent & Trademark Office
Patent Public Search | Text View

United States Patent	12393941
Kind Code	B2
Date of Patent	August 19, 2025
Inventor(s)	Hefetz; Guy et al.

Method for authenticating internet users

Abstract

A method for authenticating the identity of a user who is attempting to access a website or conduct a transaction is described. The method involves receiving two geographical locations, and associated time stamps, of a mobile phone associated with the user, one of the locations being the location of the transaction or access attempt. The method determines whether the speed required to travel between the two geographical locations in the elapsed time is within acceptable limits. A confidence score, derived in part from this calculation, is taken into account when deciding whether to allow or deny the access or the transaction.

Inventors: **Hefetz; Guy (Boca Raton, FL), Heffez; Jacob (Holon, IL), Wood; Christopher (Arlington, VA)**

Applicant: **Spriv LLC** (New York, NY)

Family ID: **1000008768257**

Assignee: **Spriv LLC (New York, NY)**

Appl. No.: **18/923969**

Filed: **October 23, 2024**

Prior Publication Data

Document Identifier	Publication Date
US 20250069077 A1	Feb. 27, 2025

Related U.S. Application Data

continuation parent-doc US 18741641 20240612 US 12260407 child-doc US 18923969
continuation parent-doc US 18482880 20231008 US 12086803 child-doc US 18741641
continuation-in-part parent-doc US 17592528 20220204 US 11818287 20231114 child-doc US 18482880
continuation-in-part parent-doc US 16724361 20191222 US 11308477 20220419 child-doc US

17592528
continuation-in-part parent-doc US 15787805 20171019 US 10521786 20191231 child-doc US 16724361
continuation-in-part parent-doc US 15606270 20170526 US 10289833 20190514 child-doc US 15787805
continuation-in-part parent-doc US 14835707 20150825 US 9391985 20161207 child-doc US 15134545
continuation-in-part parent-doc US 14479266 20140905 ABANDONED child-doc US 14835707
continuation-in-part parent-doc US 14145862 20131231 US 9033225 20150519 child-doc US 14479266
continuation-in-part parent-doc US 13479235 20120523 US 8770477 20140807 child-doc US 14145862
continuation-in-part parent-doc US 13065691 20110328 US 8640197 20140128 child-doc US 13479235
continuation-in-part parent-doc US 12260065 20081028 ABANDONED child-doc US 13065691
continuation-in-part parent-doc US 11346240 20060203 US 7503489 20090317 child-doc US 12260065
continuation-in-part parent-doc US 12357380 20090121 US 8656458 20140218 child-doc US 13065691 20110328
continuation-in-part parent-doc US 11405789 20060418 US 8590007 20131119 child-doc US 12357380
continuation-in-part parent-doc US 12600808 US 8370909 20130205 WO PCT/US2007/012552 20070529 child-doc US 13065691 20110328
continuation-in-part parent-doc US 13290988 20111107 US 8413898 20130409 child-doc US 13479235 20120523
division parent-doc US 15134545 20160421 US 9727867 20170808 child-doc US 15606270
division parent-doc US 12260065 20081028 ABANDONED child-doc US 13290988
us-provisional-application US 61445860 20110223
us-provisional-application US 61318329 20100328
us-provisional-application US 60711346 20050825

Publication Classification

Int. Cl.: **G06K5/00** (20060101); **G06Q20/32** (20120101); **G06Q20/40** (20120101); **H04W12/12** (20210101); H04W4/021 (20180101); H04W4/14 (20090101)

U.S. Cl.:

CPC **G06Q20/40** (20130101); **G06Q20/32** (20130101); **G06Q20/322** (20130101); **G06Q20/3224** (20130101); **G06Q20/401** (20130101); **G06Q20/4014** (20130101); **G06Q20/4016** (20130101); **H04W12/12** (20130101); H04W4/021 (20130101); H04W4/14 (20130101)

Field of Classification Search

CPC: G06Q (20/40); G06Q (20/401); G06Q (20/20); G06Q (20/4014); G06Q (20/32); G06Q (20/232)

USPC: 235/380; 235/382; 235/385

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
5327144	12/1993	Stilip	N/A	N/A
5335278	12/1993	Matchett	N/A	N/A
5365451	12/1993	Wang	N/A	N/A
5535431	12/1995	Grube	N/A	N/A
5754657	12/1997	Schipper	N/A	N/A
5757916	12/1997	Macdoran	N/A	N/A
5790074	12/1997	Rangedahl	N/A	N/A
5945944	12/1998	Krasner	N/A	N/A
6012144	12/1999	Pickett	N/A	N/A
6097938	12/1999	Paxson	N/A	N/A
6236365	12/2000	LeBlanc	N/A	N/A
6442485	12/2001	Evans	N/A	N/A
6466779	12/2001	Moles	N/A	N/A
6560461	12/2002	Fomukong et al.	N/A	N/A
6612488	12/2002	Suzuki	N/A	N/A
6625456	12/2002	Busso	N/A	N/A
6771969	12/2003	Chinoy	N/A	N/A
6882313	12/2004	Fan	N/A	N/A
6975941	12/2004	Lau et al.	N/A	N/A
6978023	12/2004	Dacosta	N/A	N/A
7013149	12/2005	Vetro	N/A	N/A
7080402	12/2005	Bates	N/A	N/A
7212806	12/2006	Karaoguz	N/A	N/A
7305245	12/2006	Alizadeh-Shabdiz	N/A	N/A
7321775	12/2007	Maanoja	N/A	N/A
7376431	12/2007	Niedermeyer	N/A	N/A
7418267	12/2007	Karaoguz	N/A	N/A
7450930	12/2007	Williams	N/A	N/A
7497374	12/2008	Helsper	N/A	N/A
7503489	12/2008	Heffez	N/A	N/A
7577665	12/2008	Ramer	N/A	N/A
7591020	12/2008	Kammer	N/A	N/A
7594605	12/2008	Aaron	N/A	N/A
7598855	12/2008	Scalisi	N/A	N/A
7647164	12/2009	Reevs	N/A	N/A
7669759	12/2009	Zettner	N/A	N/A
7673032	12/2009	Augart	N/A	N/A
7673793	12/2009	Greene	N/A	N/A
7751829	12/2009	Masuoka	N/A	N/A
7764231	12/2009	Karr	N/A	N/A
7769396	12/2009	Alizadeh-Shabdiz	N/A	N/A
7788134	12/2009	Manber	N/A	N/A
7832636	12/2009	Heffez	N/A	N/A
7848760	12/2009	Caspi	N/A	N/A
7865181	12/2010	Macaluso	N/A	N/A

7907529	12/2010	Wisely	N/A	N/A
7908645	12/2010	Varghese	N/A	N/A
7925273	12/2010	Fomukong et al.	N/A	N/A
8006190	12/2010	Quoc	N/A	N/A
8006289	12/2010	Hinton	N/A	N/A
8285639	12/2011	Eden	N/A	N/A
8295898	12/2011	Ashfield	N/A	N/A
8321913	12/2011	Turnbull	N/A	N/A
8370340	12/2012	Liang	N/A	N/A
8370909	12/2012	Heffez	N/A	N/A
8374634	12/2012	Dankar	N/A	N/A
8384555	12/2012	Rosen	N/A	N/A
8572391	12/2012	Golan	N/A	N/A
8606299	12/2012	Fok	N/A	N/A
8611919	12/2012	Barnes, Jr.	N/A	N/A
8640197	12/2013	Heffez	N/A	N/A
8668568	12/2013	Denker	N/A	N/A
8676684	12/2013	Newman	N/A	N/A
8739278	12/2013	Varghese	N/A	N/A
8770477	12/2013	Hefetz	N/A	N/A
8793776	12/2013	Jackson	N/A	N/A
8904496	12/2013	Bailey	N/A	N/A
8977284	12/2014	Reed	N/A	N/A
9014666	12/2014	Bentley	N/A	N/A
9033225	12/2014	Hefetz	N/A	N/A
9391985	12/2015	Hefetz	N/A	N/A
9413805	12/2015	Sainsbury	N/A	N/A
9473511	12/2015	Arunkumar	N/A	N/A
9576119	12/2016	McGeehan	N/A	N/A
9654477	12/2016	Kotamraju	N/A	N/A
9727867	12/2016	Heffez	N/A	N/A
10289833	12/2018	Hefetz	N/A	N/A
10521786	12/2018	Hefetz	N/A	N/A
10552583	12/2019	Piccionelli	N/A	N/A
10554645	12/2019	Hefetz	N/A	N/A
10645072	12/2019	Heffez	N/A	N/A
11122418	12/2020	Mullen	N/A	N/A
2001/0034718	12/2000	Shaked	N/A	N/A
2002/0016831	12/2001	Peled	N/A	N/A
2002/0019699	12/2001	McCarty	N/A	N/A
2002/0035622	12/2001	Barber	N/A	N/A
2002/0053018	12/2001	Ota	N/A	N/A
2002/0073044	12/2001	Singhal	N/A	N/A
2002/0089960	12/2001	Shuster	N/A	N/A
2002/0188712	12/2001	Caslin	N/A	N/A
2003/0009594	12/2002	McElligott	N/A	N/A
2003/0056096	12/2002	Albert	N/A	N/A
2003/0061163	12/2002	Durfield	N/A	N/A
2003/0065805	12/2002	Barnes	N/A	N/A
2003/0101134	12/2002	Liu	N/A	N/A

2003/0134648	12/2002	Reed et al.	N/A	N/A
2003/0135463	12/2002	Brown	N/A	N/A
2003/0144952	12/2002	Brown	N/A	N/A
2003/0187800	12/2002	Moore	N/A	N/A
2003/0190921	12/2002	Stewart	N/A	N/A
2003/0191568	12/2002	Breed	N/A	N/A
2004/0073519	12/2003	Fast	N/A	N/A
2004/0081109	12/2003	Oishi	N/A	N/A
2004/0088551	12/2003	Dor	N/A	N/A
2004/0111640	12/2003	Baum	N/A	N/A
2004/0219904	12/2003	De Petris	N/A	N/A
2004/0230811	12/2003	Siegel	N/A	N/A
2004/0234117	12/2003	Tibor	N/A	N/A
2004/0242201	12/2003	Sasakura	N/A	N/A
2004/0254868	12/2003	Kirkland	N/A	N/A
2004/0259572	12/2003	Aoki	N/A	N/A
2005/0021738	12/2004	Goeller	N/A	N/A
2005/0022119	12/2004	Kraemer	N/A	N/A
2005/0027543	12/2004	Yannis	N/A	N/A
2005/0027667	12/2004	Kroll	N/A	N/A
2005/0065875	12/2004	Beard	N/A	N/A
2005/0066179	12/2004	Seidlein	N/A	N/A
2005/0075985	12/2004	Cartmell	N/A	N/A
2005/0086164	12/2004	Kim	N/A	N/A
2005/0143916	12/2004	Kim	N/A	N/A
2005/0144449	12/2004	Voice	N/A	N/A
2005/0144450	12/2004	Voice	713/169	H04L 63/08
2005/0159173	12/2004	Dowling	N/A	N/A
2005/0160280	12/2004	Caslin	N/A	N/A
2005/0180395	12/2004	Moore	N/A	N/A
2005/0198218	12/2004	Tasker	N/A	N/A
2005/0268107	12/2004	Harris	713/182	H04L 63/0853
2005/0269401	12/2004	Spitzer	235/380	G07F 7/0886
2006/0020812	12/2005	Steinberg	N/A	N/A
2006/0031830	12/2005	Chu	N/A	N/A
2006/0064374	12/2005	Helsper	N/A	N/A
2006/0085310	12/2005	Mylet	N/A	N/A
2006/0085357	12/2005	Pizarro	N/A	N/A
2006/0090073	12/2005	Steinberg	N/A	N/A
2006/0107307	12/2005	Knox	N/A	N/A
2006/0128397	12/2005	Choti	N/A	N/A
2006/0194592	12/2005	Clough	N/A	N/A
2006/0217131	12/2005	Farshid	N/A	N/A
2006/0277312	12/2005	Hirsch	N/A	N/A
2006/0282285	12/2005	Helsper	N/A	N/A
2007/0053306	12/2006	Stevens	N/A	N/A
2007/0055672	12/2006	Stevens	N/A	N/A
2007/0055684	12/2006	Stevens	N/A	N/A

2007/0055732	12/2006	Stevens	N/A	N/A
2007/0055785	12/2006	Stevens	N/A	N/A
2007/0061301	12/2006	Ramer	N/A	N/A
2007/0084913	12/2006	Weston	N/A	N/A
2007/0133487	12/2006	Wang	N/A	N/A
2007/0136573	12/2006	Steinberg	N/A	N/A
2007/0174082	12/2006	Singh	N/A	N/A
2008/0046367	12/2007	Billmaier	N/A	N/A
2008/0046988	12/2007	Baharis	N/A	N/A
2008/0132170	12/2007	Farshid	N/A	N/A
2008/0146193	12/2007	Bentley	N/A	N/A
2008/0189776	12/2007	Constable	N/A	N/A
2008/0222038	12/2007	Eden	N/A	N/A
2008/0248892	12/2007	Walworth	N/A	N/A
2008/0249939	12/2007	Veenstra	N/A	N/A
2009/0172402	12/2008	Tran	705/40	G06Q 20/388
2009/0260075	12/2008	Gedge	N/A	N/A
2009/0276321	12/2008	Krikorian	N/A	N/A
2010/0051684	12/2009	Powers	N/A	N/A
2010/0057623	12/2009	Kapur	705/72	G06Q 20/12
2011/0185406	12/2010	Hirson	726/5	H04W 12/068
2011/0211494	12/2010	Rhodes	N/A	N/A
2013/0091544	12/2012	Oberheide	N/A	N/A
2013/0104198	12/2012	Grim	N/A	N/A
2013/0197998	12/2012	Buhrmann	N/A	N/A
2013/0312078	12/2012	Oberheide	N/A	N/A
2014/0068723	12/2013	Grim	N/A	N/A
2014/0245379	12/2013	Oberheide	N/A	N/A
2014/0245389	12/2013	Oberheide	N/A	N/A
2014/0245450	12/2013	Oberheide	N/A	N/A
2015/0040190	12/2014	Oberheide	N/A	N/A
2015/0046989	12/2014	Oberheide	N/A	N/A
2015/0046990	12/2014	Oberheide	N/A	N/A
2015/0054639	12/2014	Rosen	N/A	N/A
2015/0074408	12/2014	Oberheide	N/A	N/A
2015/0074644	12/2014	Oberheide	N/A	N/A
2015/0161378	12/2014	Oberheide	N/A	N/A

FOREIGN PATENT DOCUMENTS

Patent No.	Application Date	Country	CPC
1469368	12/2003	EP	N/A
1696626	12/2005	EP	N/A
1708527	12/2005	EP	N/A
1875653	12/2007	EP	N/A
2383497	12/2002	GB	N/A
2402792	12/2003	GB	N/A
1020030043886	12/2002	KR	N/A

20040095363	12/2003	KR	G06Q 20/023
20040095363	12/2003	KR	N/A
WO1996041488	12/1995	WO	N/A
WO2000075760	12/1999	WO	N/A
WO2001028272	12/2000	WO	N/A
WO2001054091	12/2000	WO	N/A
WO2002093502	12/2001	WO	N/A
WO2004/079499	12/2003	WO	N/A
WO/2004/095857	12/2003	WO	N/A
2005071988	12/2004	WO	N/A
WO2007004224	12/2006	WO	N/A

OTHER PUBLICATIONS

K. Charlton, N. Taylor, “Online Credit Card Fraud against Small Businesses”, Australian Institute of Criminology, Research and Public Policy Series, No. 60; pp. 14-20. https://www.aic.gov.au/publications/rpp/rpp60. cited by applicant

Dorothy E.Denning, Peter F.Macdoran: “Location-based authentication: grounding cyberspace for better security”, Computer Fraud and Security, Oxford, GB, (Feb. 1, 1996) XP-002117683 https://www.sciencedirect.com/science/article/abs/pii/S136137239782613 9?via%3Dihub. cited by applicant

Hideyuki Takamizawa and Noriko Tanaka: International Journal of Computer Theory and Engineering vol. 4, No. 2, Apr. 2012: “Authentication System Using Location Information on iPad or Smartphone.” http://www.ijcte.org/papers/441-A075.pdf. cited by applicant

Terry Sweeney; “SIS Taps Mobiles to Reduce Credit Fraud”; Mar. 5, 2008 05:09 PM; paragraphs 1 2 and 3 https://www.informationweek.com/sis-taps-mobiles-to-reduce-credit-fraud/d/d-id/1065356?. cited by applicant

Newbury Networks WiFi Workplace, Jun. 19, 2004, “Enterprise WLAN Management & Security”, pp. 3-4. http://www.newburynetworks.com/downloads/WiFiWorkplace.pdf via archive.org. cited by applicant

Newbury Networks WiFi Workplace, Jun. 18, 2004, “WiFiWatchdog”, pp. 2-3. http://www.newburynetworks.com:80/downloads/WifiWatchDog_DataSeet.PDF via archive.org. cited by applicant

Thomas Mundt: “Two Methods of Authenticated Positioning.” Oct. 2, 2006; University of Rostock Institute of Computer Science. pp. 1, 3, 4. cited by applicant

Bill N. Schilit et al., 2003, “Challenge: Ubiquitous Location-Aware Computing and the “Place Lab” Initiative”, Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Service Hotspots; Sep. 19, 2003, San Diego CA, pp. 29-35. cited by applicant

Sybren A. Stuvel: “Sadako—Securing a building using IEEE 802.11” Jun. 16, 2006; Universiteit van Amsterdam; p. 7. cited by applicant

cyota.com (via Archive.org): Cyota Esphinx, 2006 http://www.cyota.com/product_7.asp; http://www.cyota.com/product_7_19.asp; http://www.cyota.com/product_11_26.asp; http://www.cyota.com/product_11_25.asp. cited by applicant

Debopam Acharya, Nitin Prabhu, and Vijay Kumar: “Discovering and Using Web Services in M-Commerce” 2005; SCE, Computer Networking, University of Missouri-Kansas City. Springer-Verlag Berlin Heidelberg 2005. pp. 13-14. cited by applicant

Jeyanthi Hall: “Detection of Rogue Devices in Wireless Networks.” Aug. 2006; Ottawa-Carleton Institute for Computer Science, School of Computer Science, Carleton University Ottawa, Ontario; Abstract, pp. 10, 91, 92, 98-100, 143, 203, 205, 208. cited by applicant

Jakob E. Bardram, Rasmus E. Kjær, and Michael Ø. Pedersen: “Context-Aware User Authentication—

Supporting Proximity-Based Login in Pervasive Computing" 2003; Springer-Verlag Berlin Heidelberg 2003; Department of Computer Science, University of Aarhus. pp. 111-113, 119. cited by applicant
Adelstein et al., "Physically Locating Wireless Intruders", Journal of Universal Computer Science, vol. 11, No. 1 (2005); pp. 3, 4, 5, 6, 14. cited by applicant
CyberAngel (via Archive.org): CyberAngel Security Software White Paper http://www.thecyberangel.com/pdfs/CyberAngelWhitePaper.pdf: Feb. 17, 2006; pp. 5, 7, 17, 18, 31. cited by applicant
Kenya Nishiki and Erika Tanaka: "Authentication and Access Control Agent Framework for Context-Aware Services." 2005; Systems Development Laboratory, Hitachi, Ltd. Computer Society. pp. 1-4. cited by applicant
Business Wire: "Newbury Networks Introduces RF Firewall for Location-Based Access Control and Policy Enforcement": May 21, 2007; Las Vegas. pp. 1-2. cited by applicant
Wayne Jansen Serban Gavrila and Vlad Korolev: "Proximity Beacons and Mobile Device Authentication: An Overview and Implementation." Jun. 2005; National Institution of Standards and Technology. US Department of Commerce. Abstract, pp. 1-2, 7, 19. cited by applicant
PR Newswire: "Interlink Networks and Bluesoft Partner to Deliver Wi-Fi Location-Based Security Solutions" Apr. 24, 2003. PRNewswire Ann Arbor, Mich. and San Mateo, Calif. p. 1. cited by applicant
Paul C. Van Oorschot, S. Stubblebine: "Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling" Feb. 28-Mar. 3, 2005 Financial Cryptography and Data Security 9th International Conference, FC 2005 Roseau, The Commonwealth of Dominica. pp. 3, 6, 7, 11-13. cited by applicant
Shashwat V. Bhavsar: "Wireless Application Environments and Location-Aware Push Services" Dec. 2005; University of New Brunswick. pp. 119, 123, 138-142, 150, 152, 153,. cited by applicant
Simon G. M. Koo, Catherine Rosenberg, Hoi-Ho Chan, and Yat Chung Lee: "Location-based E-campus Web Services: From Design to Deployment" 2003. School of Electrical and Computer Engineering and Center for Wireless Systems and Applications, Purdue University, West Lafayette, IN 47907-1285, pp. 4, 5, 7. cited by applicant
MaxMind (via archive.org): "Skyhook Wireless and MaxMind Announce Partnership", Jan. 30, 2006, p. 1. http://www.maxmind.com/app/news_20060130. cited by applicant
Maxmind (via archive.org): "Maxmind minFraud", Jan. 8, 2007. pp. 1-2. https://www.maxmind.com/MaxMind_minFraud_Overview.pdf. cited by applicant
CyberAngel (via archive.org): Jun. 20, 2005; "CyberAngel Security Solutions and Skyhook Wireless Announce Groundbreaking New Laptop Recovery System" pp. 1,2. http://www.thecyberangel.com/pr/TheCA_SkyhookPart.pdf. cited by applicant
RSA Security (via Archive.org): "RSA Adaptive Authentication the Logical Consumer Solution" p. 2. Mar. 14, 2006 http://www.rsasecurity.com/solutions/consumer_authentication/ADAPT_SB_0106.pdf. cited by applicant
RSA Security (via Archive.org): RSA Adaptive Authentication for web; https://web.archive.org/web/20061230232715/http://www.rsasecurity.com/node.asp?id=3018 (archived Dec. 30, 2006). cited by applicant
Cyota (via archive.org): "Cyota eSphinx—How does it work?" https://web.archive.org/web/20060324224711/http://www.cyota.com//product_7_19.asp (Archived Mar. 24, 2006). cited by applicant
RSA Security (via Archive.org): "RSA eFraudNetwork" http://www.rsasecurity.com/node.asp?id=3071 (Archived Dec. 10, 2006). cited by applicant
Sharma "Location based authentication" M.S. Thesis, University of New Orleans, May 20, 2005. pp. 17-25 https://scholarworks.uno.edu/td/141. cited by applicant
Lenders, V. et al., "Location-Based Trust for Mobile User-granted Content: Applications, Challenges and Implementations", HotMobile '08: Proceedings of the 9th workshop on Mobile computing systems and applications, Napa Valley, CA Feb. 25-26, 2008, pp. 60-64. cited by applicant

Epaynews, “Security System Matches Card Purchase to Cellphone Location.” ePaynews, the Payment News and Resource Center. Mar. 12, 2008 https://www.atmmarketplace.com/news/security-system-matches-card-purchase-to-cell-phone-location/. cited by applicant
Chen, Y. et al., “Cache Management Techniques for Privacy Preserving Location-based Services” Dept. of Electrical & Computer Engineering, SUNY—Binghamton, Binghamton, NY 13902 https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.417.3047&rep=rep1&type=pdf. cited by applicant
“Maxmind, Online Guidelines for Preventing Online Credit Card Fraud” http://web.archive.org/web/20050516073510/http://www.maxmind.com/app/prevent_credit_card_fraud May 12, 2005. cited by applicant

---

Primary Examiner: St. Cyr; Daniel

Attorney, Agent or Firm: Cittone Demers & Arneri LLP

Background/Summary

CROSS-REFERENCE TO RELATED APPLICATIONS (1) This application is a continuation of U.S. patent application Ser. No. 18/741,641, filed Jun. 12, 2024, now U.S. Pat. No. 12,260,407, which is a continuation of U.S. patent application Ser. No. 18/482,880, filed Oct. 8, 2023, now U.S. Pat. No. 12,086,803, which is a continuation-in-part of U.S. patent application Ser. No. 17/592,528, filed Feb. 4, 2022, now U.S. Pat. No. 11,818,287, which is a continuation-in-part of U.S. patent application Ser. No. 16/724,361, filed Dec. 22, 2019, now U.S. Pat. No. 11,308,477. (2) Application Ser. No. 16/724,361 is a continuation-in-part of U.S. patent application Ser. No. 15/787,805, filed Oct. 19, 2017, now U.S. Pat. No. 10,521,786, which is a continuation-in-part of U.S. patent application Ser. No. 15/606,270, filed May 26, 2017, now U.S. Pat. No. 10,289,833, which is a continuation-in-part of U.S. patent application Ser. No. 15/134,545, filed Apr. 21, 2016, now U.S. Pat. No. 9,727,867, which is a continuation-in-part of U.S. patent application Ser. No. 14/835,707, filed Aug. 25, 2015, now U.S. Pat. No. 9,391,985, which is a continuation-in-part of U.S. patent application Ser. No. 14/479,266, filed Sep. 5, 2014 and now abandoned. (3) Application Ser. No. 14/479,266 is a continuation-in-part of U.S. patent application Ser. No. 14/145,862, filed Dec. 31, 2013, now U.S. Pat. No. 9,033,225, which is a continuation-in-part of U.S. patent application Ser. No. 13/479,235, filed May 23, 2012, now U.S. Pat. No. 8,770,477, which is a continuation-in-part of U.S. patent application Ser. No. 13/065,691 filed Mar. 28, 2011, now U.S. Pat. No. 8,640,197, which is a continuation-in-part of U.S. patent application Ser. No. 12/260,065 filed on Oct. 28, 2008 and now abandoned, which is a continuation-in-part of U.S. patent application Ser. No. 11/346,240 filed on Feb. 3, 2006, now U.S. Pat. No. 7,503,489, which in turn claims priority from U.S. provisional application No. 60/674,709, filed Apr. 26, 2005. (4) U.S. patent application Ser. No. 13/065,691 is also a continuation-in-part of U.S. patent application Ser. No. 12/357,380, filed on Jan. 21, 2009, now U.S. Pat. No. 8,656,458, which is a continuation-in-part of U.S. patent application Ser. No. 11/405,789 filed on Apr. 18, 2006, now U.S. Pat. No. 8,590,007, which in turn claims priority from U.S. provisional application No. 60/711,346 filed on Aug. 25, 2005. (5) U.S. application Ser. No. 13/065,691 is also a continuation-in-part of U.S. patent application Ser. No. 12/600,808, filed on May 29, 2007, now U.S. Pat. No. 8,370,909, which in turn is a 371 (National Stage in the US) of PCT/US07/012552 filed May 29, 2007. (6) U.S. application Ser. No. 13/479,235 is also a continuation-in-part of U.S. patent application Ser. No. 13/290,988, filed on Nov. 7, 2011, now U.S. Pat. No. 8,413,898, which in turn is a divisional of

U.S. application Ser. No. 12/260,065, supra. (7) The entire contents of all of the above-referenced applications are incorporated herein by reference.

FIELD OF THE INVENTION

(1) This invention relates to a method and system for monitoring electronic purchases.

BACKGROUND OF THE INVENTION

(2) As credit card and debit card purchases have expanded both in number and in the methods by which they can be accomplished, particularly electronic purchases, the opportunity for fraudulent, invalid or unauthorized purchases has increased. The expansion of such purchase opportunities has resulted in an increase in monetary losses to sellers, merchants, financial institutions and authorized holders of the authorized credit card and debit cards. In response, methods and systems have been developed to reduce the number of fraudulent purchases through verification processes and systems.

(3) An example of a method of increasing the security of payments made by credit and cash cards is set forth in U.S. Patent Publication No. 20040073519.

(4) Another example of a method of increasing the security of payments made by credit and cash cards is set forth in U.S. Patent Publication No. 20040254868.

(5) A cellular telephone location system for automatically recording the location of one or more mobile cellular telephones is described, for example, in U.S. Pat. No. 5,327,144. The system comprises a central site system operatively coupled to at least three cell sites. Each of the cell sites receives cellular telephone signals and integrates a timing signal common to all the cell sites. The central site calculates differences in times of arrival of the cellular telephone signals arriving among the cell sites and thereby calculates the position of the cellular telephone producing the cellular telephone signals. Additional examples of known methods for locating phones are cell sector and cell site. The full disclosure of U.S. Pat. No. 5,327,144 is hereby incorporated by reference in its entirety.

(6) The Federal Communications Commission (FCC) has recently mandated wireless Enhanced 911 (E911) rules to improve the effectiveness and reliability of wireless 911 service by providing 911 dispatchers with additional information on wireless 911 calls. According to the FCC website, the wireless E911 program is divided into two part-Phase I and Phase II. Phase I requires carriers, upon appropriate request by a local Public Safety Answering Point (PSAP), to report the telephone number of a wireless 911 caller and the location of the antenna that received the call. Phase II requires wireless carriers to provide far more precise location information, within 50 to 300 meters in most cases. The deployment of E911 requires the development of new technologies and upgrades to local 911 PSAPs, as well as coordination among public safety agencies, wireless carriers, technology vendors, equipment manufacturers, and local wireline carriers. The FCC established a four-year rollout schedule for Phase II, beginning Oct. 1, 2001 and to be completed by Dec. 31, 2005.

SUMMARY OF THE INVENTION

(7) A method for facilitating the detection of misuse of an identity during an electronic transaction. The present invention comprises at least five embodiments. In a first embodiment, the method comprises the steps of: receiving a notification to authenticate the use of an identity at a first location, wherein the identity is associated with a first wireless terminal; determining an approximate location of the first wireless terminal based on cached position information, the approximate location of the first wireless terminal being a second location; determining whether the first and second locations match in geographical proximity; and generating an alert if the first and second locations do not match in geographical proximity. In a second embodiment, an approximate location of the first wireless terminal is determined based on cached position information stored on a GPS position database.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

(1) FIG. **1** is a schematic block diagram showing exemplary hardware elements that can enable the practice of the various embodiments of the present invention.

(2) FIG. **2** shows a schematic block diagram of an exemplary first wireless terminal fitted with a GPS receiver operatively coupled to an inertial navigation system according to one aspect of the present invention.

(3) FIG. **3** shows a non-limiting example of a user registration process according to one aspect of the present invention.

(4) FIG. **4** shows a non-limiting flow chart of one embodiment of the invention.

(5) It should be understood that the attached figures are not intended to limit the scope of the present invention in any way.

DETAILED DESCRIPTION OF THE INVENTION

(6) This invention relates to a method and system for monitoring electronic transactions. In general terms, in one aspect of the invention a user identity (such as the user's credit card, cash card, etc.) is associated with a first wireless terminal, e.g., the user's cell phone. The position of the user's cell phone is determined at intervals and cached (i.e., archived) to provide a stream of regularly updated pre-transaction positions. Each cached pre-transaction position can be stored on a remote position database (PDB) or on the user's cell phone. If the user's identity such as the user's credit or cash card is later used, for example, at a point of sale (POS) electronic terminal having a known location (being a first location), the invention detects the use of the user's credit card (i.e., identity) at the first location and compares the first location with the most recent cached position of the user's cell phone (now treated as a pre-transaction position to provide a second location for comparison). Specifically, a determination is made as to whether the first and second locations match in geographical proximity. If the first and second locations do not match in geographical proximity, the invention generates an alert or advisory message that is communicated to a predetermined notification device, such as the user's email account, a POS electronic terminal, a financial institution's computers or offices (such as the user's credit card company's computers, etc.). The alert can also be a reply message for blocking an associated electronic transaction at the first location.

(7) The invention can be adjusted such that as each new pre-transaction position corresponding to the user's cell phone becomes available, the new pre-transaction position can be used to overwrite the currently archived pre-transaction position to prevent illicit or unauthorized tracking of the user's movements.

(8) In another aspect of the invention, if the latest archived pre-transaction location (i.e., second location) and known POS location (i.e., first location) don't match, a post-transaction position (being a third location) of the user's cell phone is obtained and compared to the known first location and an alert generated if the post-transaction location (third location) and known POS location (first location) do not match in geographical proximity. Such matching can be based on a predetermined distance. For example, if the post-transaction location of the user's cell phone is determined to be more than **5** miles from the known POS location, an alert is generated and communicated to a predetermined device such as the user's cell phone and/or email address, and/or to an appropriate financial institution such as the user's bank or a credit card company's computers, the user's wireless personal digital assistant or a user's wireless enabled laptop, etc. Thus, if the actual position of the user's cell phone is not available at about the time of the transaction, the pre or post-transaction position of the user's cell phone can be used to determine if an alert is warranted.

(9) For example, the user's cell phone may include a GPS receiver capable of determining the position of the user's cell phone, but only if the user's GPS capable cell phone is able to receive

GPS signals necessary to calculate the location of the user's cell phone. GPS signals are transmitted by dedicated satellites and are often not strong enough to be received inside buildings where many ATM and POS terminals are located. The invention provides a non-obvious way of monitoring the use of one or more identities (such as a credit card or cash card number) associated with a user regardless of the ability of a user's cell phone to pick up GPS signals at the time of transaction (i.e., when the user's identity is used to authorize a transaction).

(10) Specifically, through such monitoring, the invention facilitates the detection of a possible fraudulent or an invalid electronic purchase involving the use of a user's identity, for example, a credit card, debit card or any other kind of electronic payment or purchase system including biometric based purchases. Upon detection of suspect purchase or transaction (such as a cash withdrawal at an ATM), an advisory message is communicated to a predetermined notification device. The intent of this invention is to provide an alert upon detection of an inappropriate purchase or transaction.

(11) The invention is now described in more detail.

(12) It should be understood that the term “wireless terminal” (and its derivatives such as “first wireless terminal”), as used in the context of the present invention, applies to any device capable of communicating with a wireless network or cellular system. A non-limiting example of a first wireless terminal includes a cellular telephone (sometimes referred to as a cell phone or a wireless phone). Other non-limiting examples include any device that has been modified or designed to communicate with a wireless network including, but not limited to: a Personal Digital Assistant (“PDA”), such as a WiFi capable PDA, or a wireless Blackberry (such as the Blackberry 7520 model).

(13) The predetermined notification device can be any suitable device capable of receiving communications directly or indirectly from a wireless network, such as, but not limited to: a first mobile terminal, a second mobile terminal, a Personal Digital Assistant (PDA) capable of communicating with a wireless network, a laptop computer capable of communicating with a wireless network, a message server, and an email server, an electronic terminal **120**, alone or in combination. An alert sent to an electronic terminal **120** at the first location, wherein the alert prevents a transaction associated with the identity

(14) The position of a mobile terminal can be determined by, for example, an internal positioning apparatus and an external position apparatus, alone or in combination. Examples of internal positioning apparatus include a GPS receiver built into the mobile terminal that receives Global Positioning System (“GPS”) radio signals transmitted from GPS satellites. The GPS system can be supplemented with an INS (inertial navigation system) also built into the mobile terminal (see FIG. **2**).

(15) The external positioning apparatus can be a cellular positioning system that computes the position of the mobile terminal by observing time differences among the arrivals of a radio signal transmitted by the mobile terminal at a plurality of observation points, i.e., base stations, which typically form part of the wireless network. Alternatively, the external positioning apparatus could be a single base station that the mobile terminal is in contact with. Each base station has a particular base station ID and a location associated with the base station ID. Thus, the location of a mobile terminal can be approximated to the actual location of a base station, but given that the typical area covered by a base station is often about one kilometer, it is difficult to accurately determine the position of the mobile terminal.

(16) The role of base stations in wireless networks is described, for example, in “Cellular Radio Systems”, published by Artech House, Boston (editors: D. M. Balston and R. C. V. Macario; ISBN: 0-89006-646-9); “Digital Cellular Radio” written by G. Calhoun and published by Artech House, Boston (ISBN: 0-89006-266-8). “Cellular Radio Systems” and “Digital Cellular Radio” are hereby incorporated by reference in their entirety.

(17) The position of a mobile terminal can also be tracked using external RFID tags (Radio

Frequency Identification tags) in combination with an RFID reader built into the mobile terminal. How RFID tags and readers work is described in U.S. Patent Publication No. 20050143916 published Jun. 30, 2005 to Kim, In-Jun, et al. U.S. Patent Publication No. 20050143916 is incorporated by reference herein in its entirety.

(18) In a first embodiment of the present invention, a method is provided for facilitating the detection of misuse of an identity during an electronic transaction. The first embodiment comprises the steps of: receiving a notification to authenticate the use of an identity at a first location, wherein the identity is associated with a first wireless terminal; determining an approximate location of the first wireless terminal based on cached position information, the approximate location of the first wireless terminal being a second location; determining whether the first and second locations match in geographical proximity; and generating an alert if the first and second locations do not match in geographical proximity.

(19) The cached position information can be cached GPS position information stored on the first wireless terminal. The step of determining the second location can further comprise the step of updating the cached position information with an inertial navigation system correction performed by the first wireless terminal to provide an updated location of the first wireless terminal, the updated location being the second location.

(20) In one aspect of the first embodiment, the step of determining the second location further comprises the step of detecting whether GPS signals are being received by the first wireless terminal to determine a post-transaction location of the first wireless terminal, the post-transaction location being the second location. The step of detecting whether sufficient GPS signals are being received by the first wireless terminal for the first terminal to determine a post-transaction is only performed if cached position information is not stored on the first wireless terminal or if the cached position information is stale. The cached position information is regarded as stale if the information has not been updated for a predetermined time period, e.g., has not been within the last 30 minutes, 15 minutes or last 5 minutes. The predetermined time period defining when the cached position information is stale can vary and may be factory set or optionally set by the owner or user of the identity.

(21) The first wireless terminal can be any device that can wirelessly communicate with a network, such as a cell phone, which can communicate wirelessly with a wireless network. Examples of suppliers of cell phones are Nokia, Motorola, and Ericsson. The terms “cell” and “cellular” are regarded as equivalent terms.

(22) The identity can be a credit card number, an account number, a debit card identification number, a driver's license number, a name and address, a social security number, a telephone number, a finger print, an iris scan identity, a retina scan identity, and a membership identity (such as a membership password), alone or in combination. The identity can also be any suitable biometric identity, such as a fingerprint, an iris scan identity and a retina scan identity, alone or in combination.

(23) With respect to the notification associated with the use of the identity at the first location, the notification can be generated, for example, by an electronic transaction device (such as a credit card reader at a restaurant, an ATM machine such as a cash-withdrawal terminal that incorporates a card reader) at the first location or by, for example, a credit card company in communication with the electronic device at the first location.

(24) It should be understood that the electronic transaction device could be any suitable device where the identity can be entered for the purpose of performing an electronic transaction. For example, a credit card with a credit card number can be read by the electronic device, and the credit card number communicated to the credit card company associated with the credit card, and in response the credit card company generates a notification, which is routed to the first wireless terminal. In response to receiving the notification, the first wireless terminal determines its location based on cached position information stored on the first wireless terminal or if the cached location

information is stale requesting the first wireless terminal to provide a fresh location.
(25) Referring to the invention in general, the generated alert can take any suitable form. For example, the alert can be an advisory message, which is communicated to at least one predetermined device. The at least one predetermined device could be the first wireless terminal and/or a second wireless terminal, wherein the first wireless terminal also acting as the predetermined device could be a cell phone. The predetermined device can be any suitable device, such as a Personal Digital Assistant (PDA) and/or a laptop capable of communicating with a wireless network and/or receiving emails, and a message server. An example of a message server is a server accessible via the world-wide-web (WWW) and which stores messages for downloading by, for example, a wireless capable laptop with authorization to access the message server. The message server could be an email server programmed to store and/or forward emails to subscribers. Other examples of message servers include the hotmail email system and the webmail service provided by Google called Gmail.
(26) Alternatively, the generated alert can be routed to the user's email address recorded during a previous registration of the identity. Alternatively, the alert is a reply message, such as a non-authorization message, for blocking an associated electronic transaction at the first location, and more particularly for blocking a transaction at the first location associated with the identity. It should be understood that the identity may not be limited to one identity, but could encompass one or more identities such as a user's credit card number together with the user's email address, social security number, phone number, residential address or phone number. Thus, a card reader may read a user's credit card and the user asked to enter or otherwise provide their email address or phone number. Some retail outlets routinely ask customers for their home phone number and/or address.
(27) In one aspect of the invention, the use of an identity is associated with a first time stamp. The first time stamp corresponds to the time of the associated electronic transaction (or attempted electronic transaction) performed at a first location, and wherein the step of reading a cached location is associated with a second time stamp. The speed can be calculated based on the distance between the first and second locations and the time difference between the first and second time stamps such that the first and second locations are judged not to match in geographical proximity if the speed is above a predetermined value. Thus, if the speed to travel between the first and second locations is calculated to be about 1000 mph, and the predetermined value is set at 40 mph, an alert would be generated.
(28) In another aspect of the first embodiment, if the first and second locations do not match in geographical proximity, then a confidence score is calculated to determine if the position mismatch with respect to the first and second locations is acceptable or unacceptable, and the alert is only generated if the confidence score is below a predetermined threshold. In addition to the time and distance difference, the system can also use additional factors to derive the confidence score. These factors can be weather conditions, time of day, day of year, urban makeup (e.g. a suburb area versus a downtown area), etc.
(29) In still another aspect of the first embodiment, the step of determining the second location further comprises the step of detecting a WiFi Unique ID associated with the position of the first wireless terminal, and converting the WiFi unique ID into a post-transaction location for the first wireless terminal, the post-transaction location being the second location, wherein the step of detecting a WiFi Unique ID is only performed if cached position information is not stored on the first wireless terminal. For example, if the wireless terminal lacks cached position information and the first wireless terminal is able to detect a WiFi unique ID, then the WiFi unique ID, which is used to determine the position of the first wireless terminal. This might entail accessing a database that matches a WiFi's unique ID (i.e., identity such as, but not limited to, an Internet media-access-control (MAC) address) with known positions corresponding to each WiFi unique ID. This database might be stored, for example, on a ≤1.5″ hard drive (i.e., a less-than or equal to 1.5 inch hard drive) or on a large capacity memory chip fitted to the first wireless terminal **160**.

(30) In still another aspect of the first embodiment, the step of determining the second location further comprises the step of detecting a WiMAX Unique ID associated with the position of the first terminal, and converting the WiMAX Unique ID into a post-transaction location for the first wireless terminal, the post-transaction location being the second location, wherein the step of detecting a WiMAX Unique ID is only performed if cached position information is not stored on the first wireless terminal. Alternatively, the step of detecting a WiMAX Unique ID is only performed if the cached position information is stale, wherein the cached position information is regarded as stale if the information has not been updated for a predetermined time period.
(31) In still another aspect of the first embodiment, the step of determining the second location further comprises the step of obtaining a post-transaction position for the first wireless terminal as soon as the first wireless terminal is able to receive GPS signals to calculate its post-transaction position, the post-transaction position being the second location, wherein the step of obtaining a post-transaction position is only performed if cached position information is not stored on the first wireless terminal.
(32) In still another aspect of the first embodiment, the step of determining the second location further comprises the step of obtaining a post-transaction position for the first wireless terminal as soon as the first wireless terminal is able to receive GPS signals to calculate its post-transaction position, the post-transaction position being the second location, wherein the step of obtaining a post-transaction position is only performed if the cached position information is stale, wherein the cached position information is regarded as stale if the information has not been updated for a predetermined time period.
(33) In a second embodiment of the present invention, a method is provided for facilitating the detection of misuse of an identity during an electronic transaction. The second embodiment comprises the steps of: receiving a notification to authenticate the use of an identity at a first location, wherein the identity is associated with a first wireless terminal; determining an approximate location of the first wireless terminal based on cached position information stored on a GPS position database, wherein the GPS position database is operatively connected to a wireless provider **180** and/or a financial institution's computers **140**, the approximate location of the first wireless terminal being a second location; determining whether the first and second locations match in geographical proximity; and generating an alert if the first and second locations do not match in geographical proximity.
(34) In a third embodiment of the present invention, a method is provided for facilitating the detection of misuse of an identity during an electronic transaction, comprising the steps of: receiving a notification to authenticate the use of an identity at a first location, wherein the identity is associated with a first wireless terminal; reading a cached location of the first wireless terminal based on cached position information stored on the first wireless terminal, the location of the first wireless terminal being a second location; determining whether the first and second locations match in geographical proximity; determining a post-transaction location of the first wireless terminal if the first and second locations do not match in geographical proximity, the post-transaction location of the first wireless terminal being a third location; and generating an alert if: (1) the first and second locations do not match in geographical proximity and (2) the first and third locations do not match in geographical proximity.
(35) Referring to the invention in general and with reference to the third embodiment, the post-transaction location can be obtained, for example, by processing GPS signals received by the first wireless terminal **160** within a reasonable time after the transaction (referred to hereinafter as “post-transaction GPS signals”). Post-transaction location can also be obtained, for example, using WiFi unique ID (if available) or WiMax unique ID. Alternatively, the post-transaction location can be obtained by using an inertial navigation module (INM) **400** (discussed infra) to convert the most recent cached location into a post-transaction location for the first wireless terminal, wherein updating the most recent cached position of the INM module is integrated into the design of the

first wireless terminal (see, e.g., FIG. **3**). Thus, the post-transaction location can be determined based on a method selected from the group consisting of: processing post-transaction GPS signals, WiFi unique ID, and WiMax unique ID, and any combination thereof.

(36) In a fourth embodiment of the present invention, a method is provided for facilitating the detection of misuse of an identity during an electronic transaction, comprising the steps of: receiving a notification to authenticate the use of an identity at a first location, wherein the identity is associated with a first wireless terminal; reading a cached location of the first wireless terminal based on cached position information stored on the first wireless terminal, the location of the first wireless location being a second location; determining whether the first and second locations match in geographical proximity; determining the post-transaction location of the first wireless terminal if the first and second locations do not match in geographical proximity, the post-transaction location of the first wireless terminal being a third location; determining a post-transaction position of the first wireless terminal if (1) the first and second positions do not match in geographical proximity and (2) it is not possible to determine the post-transaction location, wherein the post-transaction position is treated as the third location; and generating an alert if: (1) the first and second locations do not match in geographical proximity and (2) the first and third locations do not match in geographical proximity.

(37) FIG. **1** is a schematic block diagram showing exemplary hardware elements that can enable the practice of the various embodiments of the present invention. An electronic transaction terminal is shown at **120**. The electronic transaction terminal **120** can be, for example, a credit and/or debit card terminal located at a first location such as a point of sale location inside a retail store, i.e., at a known first location. Alternatively, the terminal **120** could be a credit/debit card terminal linked to a cash register (not shown) or the terminal **120** could be a regular ATM (automatic teller machine) for dispensing cash to registered holders of cash cards. In other words, the terminal **120** can take various forms without detracting from the spirit of the present invention. If the first and second locations do not match in geographical proximity, the alert can be a reply message for blocking an associated electronic transaction at the first location.

(38) The terminal **120** is operatively coupled to a financial institution's computers **140** such as a credit card company's computers or a bank's computers if, for example, terminal **120** is an ATM and used for cash withdrawals). The financial institution's computers **140** are those computers authorized to process the user's financial transactions. The financial institution's computers **140** are in turn able to communicate with a first wireless terminal **160** via a wireless provider **180** and, based on signal strength, the nearest base station **170** to the first wireless terminal **160**. Examples of credit card companies include Visa, Discover, American Express, MasterCard, and Eurocard. Examples of wireless providers include Sprint, Verizon and T-Mobile.

(39) An optional position database (PDB) **300** can be operatively coupled to the wireless provider **180**. Alternatively, PDB **300** can be operatively coupled to the financial institution's computer **140**. The PDB **300** can be operatively coupled to more than one element such as wireless provider **180** and financial institution's computers **140**. The PDB **300** can be directly or indirectly linked to wireless provider **180** and/or financial institution's computers **140**. The terms “coupled” or “operatively coupled” are intended to cover both direct and indirect links. Pre-transaction and/or post-transaction positions with respect to the first wireless terminal **160** can be stored on the PDB **300**. The PDB **300** can store positions derived from any known position determination technique such as, but not limited to, GPS position data derived from a GPS receiver **200** located on the first wireless terminal **160** (see, e.g., FIG. **2**).

(40) The optional PDB **300** can, for example, archive or cache a position history of the first wireless terminal **160**. Thus, if the first wireless terminal **160** is unable to receive GPS signals or is switched off, the optional position database **300** can be accessed to provide the latest available position of the first wireless terminal **160**, i.e., in this scenario, the first wireless terminal **160** uploads its position at predetermined intervals to the wireless vendor **180** and thence to the position

database **300**.
(41) Alternatively, positions based on previously received GPS signals can be stored in a memory **320** integrated with the first wireless terminal **180**. The memory **320** can be any suitable memory such as, but not limited to: a RAM chip, a floppy disk, a hard disk drive such as an iPod battery powered 1.8-inch 60 GB hard disk drive or the anticipated 0.85 inch 3 GB hard disc drive, a CD-ROM, and a DVD-ROM, any known memory or anticipated memory option, alone or in combination.
(42) In FIG. **1**, the wireless terminal **160** is a cell phone fitted with a GPS receiver **200**. The first wireless terminal can also include memory for storing cached positions, i.e., a history of the positions of the first wireless terminal, so that if the wireless terminal is required to supply its post-transaction position but is unable to do so, perhaps because the first wireless terminal is unable to receive GPS signals, then the latest cached position can be used. The first wireless terminal **160** can be a GPS enabled cell phone as shown, or any wireless terminal capable of communication with a wireless provider such as a Blackberry in combination with a GPS receiver.
(43) Still referring to FIG. **1**, terminal **120** includes a card reader **240** for reading a credit card **260**. An identity in the form of a credit card number and details are stored on a magnetic strip **280** and are read by the card reader **240**. It should be understood that the magnetic strip **280** could be replaced with any known or future technology, e.g., a smart chip embedded in a credit or debit card, which can be read by, for example, waving the card near a card reader enabled to so read credit and/or debit cards fitted with smart chips.
(44) At any point after the identity has been read by terminal **120**, a notification can be generated by the electronic terminal **120** or other device operatively coupled to the terminal **120**, and/or the credit card company's or bank's computers **140**. One or more notifications can be generated by, for example, the electronic transaction terminal **120** and the credit card company's or bank's computers **140**, alone or in combination. The notification acts as a trigger wherein the post-transaction or cached position of the first wireless terminal **160** (treated as the second position) is determined and compared to the position of the electronic transaction terminal **120** (regarded as the first position). More specifically, a check is made to determine if the first and second positions match in geographical proximity. The task of determining if the first and second positions match in geographical proximity can be done by one or more elements such as, but not limited to, the first wireless terminal **160**, the wireless provider **180** and the computers **140**, the electronic transaction terminal **120** (or an optional processor **130** operatively coupled to the terminal **120**), alone or in combination. If the computers **140**, first wireless terminal **160**, wireless provider **180**, alone or in combination, is/are tasked to determine if the first and second positions match in geographical proximity, then the notification should include data representative of the first position of the electronic transaction terminal **120**.
(45) While wireless terminals (e.g., wireless mobile terminals such as cell phones) having a GPS receiver combined with a communication system capable of communicating with a base station are known (e.g., U.S. Pat. No. 5,945,944 describes such a device), the prior art does not teach a method and system for monitoring electronic purchases and cash-withdrawals of the present invention. U.S. Pat. No. 5,945,944, issued Aug. 31, 1999 to N. F. Krasner, is herein incorporated by reference in its entirety.
(46) In another embodiment, a GPS receiver **200** operatively coupled to a miniature inertial navigation module (INM) **400**. FIG. **2** shows a schematic block diagram of an exemplary first wireless terminal **160** fitted with a GPS receiver **200** operatively coupled to an INM **400**. The GPS receiver and INM combination can be housed inside the housing **165** of the first wireless terminal. Suppliers of miniature inertial navigation hardware include Analog Devices Inc. and Comarco, Inc. (and more particularly its subsidiary Comarco Wireless Technologies (CWT) of Irvine, Calif. 92618, USA). CWT miniature inertial modules are capable of precision position measurements in buildings and urban canyons and, when combined with a GPS receiver **200**, can determine the

position of a first wireless terminal **160** with a high degree of accuracy and reliability.
(47) INM technology in the form of silicon is available, for example, from Analog Devices Inc. (ADI). The ADI ADXL103 (a 5 mm×5 mm×2 mm LCC package), which is a high accuracy, high stability, low cost, low power, complete single axis accelerometer with a signal conditioned voltage output, all on a single monolithic IC. The ADXL213 supplied by ADI is a precision, low power, complete dual axis accelerometer with signal conditioned, duty cycle modulated outputs, on a single monolithic integrated chip (IC) measuring 5 mm×5 mm×2 mm. Also, ADI's ADXL311 is a low cost, low power, complete dual axis accelerometer with signal conditioned voltage outputs, all on a single monolithic IC of dimensions of just 5 mm×5 mm×2 mm. In addition, ADI's ADXRS401 is a low-cost complete ultra small and light (<0.15 cc, <0.5 gram) angular rate-sensing gyroscope capable of measuring up to 75 degrees per second with all of the required electronics on a single chip.
Working Example
(48) The following is a non-limiting working example of a fifth embodiment of the present invention. A credit card customer agrees to be locatable via his or her mobile phone provider and registers a credit card or debit card (hereinafter “credit card”) in such a manner that the user's credit card is associated with at least one mobile terminal. The process of registering a credit card in a Location-Based Fraud Protection (“LBFP”) System involves a financial institution which partners with one or more mobile phone or wireless providers that provide mobile geographical location(s). A mobile phone provider agrees, usually for a fee, to release the location of a subscriber who, in order to comply with privacy laws, authorizes this action. The financial institution, using the LBFP system, can register its clients using the following method (as shown in FIG. **3**): sending a letter or calling the client, and requesting the client to call a toll-free number from his cell phone. Using the caller's ID, the LBFP system will require at least two identifying numbers. These identifying numbers can be the last 4 digits of the credit card and the home address zip code. Once the customer enters these numbers, the LBFP system will communicate these details to the client's financial institution for verification. For added security, the LBFP system can also challenge the client by sending a 4-digit SMS random number to the cell phone and asking the client to enter it using his phone keypad. If verified, the LBFP system will be able to associate the correct credit card with the customer's cell phone number. The LBFP system will then check to see if the client's cell phone carrier participates in this program. If it does, the LBFP will successfully add the client to its database (as described in the next paragraph) for credit card transaction monitoring. The LBFP system can then provide an optional unique PIN to the client so that he can access the LBFP web site to further custom the alerting logic. In turn, this customization can further increase the accuracy of the LBFP system. For example, the client can add known locations to be used when an online transaction takes place. Known locations can be a work address, relative/friend's address, etc. Using these addresses will increase the LBFP accuracy when a customer uses a credit card online by comparing known locations with client's cell phone location at the approximate time of the online transaction.
(49) The financial institution stores in a database the subscriber customer (hereinafter “subscriber”) details. For example, the subscriber's first and last name (stored as a type UTF-8 characters), Mobile carrier/Wireless provider code (e.g., Sprint-1, Nextel-2) stored as type Integer number, 10-digit Mobile phone number (3-digit area code and 7-digit phone number, stored as type Integer number), and ID number that is associated with the financial institution's subscriber's ID number (stored as type Integer number), such cross-reference number acting as a security measure whereby no personal information (SSN, credit card number) is stored in such database.
(50) After registration, each time a subscriber uses the credit card, at the time of a purchase transaction or near to that time, the financial institution will contact the LBFP System servers via a secure encryption link (e.g., SSL/SSH/VPN. With no personal information of the subscriber being transmitted, the financial institution provides the date of transaction, time of transaction, address of

the business where the transaction took place, type of transaction (online or physical) and the subscriber's ID number. The LBFP servers will then initiate a request via secure TCP/IP link (e.g., SSL/SSH/VPN) to the subscriber's mobile phone provider requesting the subscriber's post-transaction location, heading and/or speed (see FIG. **4**). The actual physical location of the LBFP System does not matter. The LBFP System can be located on the financial institution's premises or at a distance therefrom. If at a distance from the LBFP System, the financial institution can be linked to it via a secure network link (e.g. VPN/SSh/SSL).

(51) When the client uses his or her credit card, the LBFP System receives the purchase information from the financial institution, it cross-references the identifying item from the financial institution with the subscriber's unique carrier ID (e.g., cell phone number).

(52) After the LBFP System finds the subscriber's unique carrier ID (or related information), it will then request the subscriber's last known location from the subscriber's carrier. Each carrier has specific means for interfacing with and providing this information. It is sometimes called API, which are known programming methods to execute specific functions. As a practical matter, the LBFP System, or the financial institution, will create a relationship and interface with the carrier ahead of time in order to obtain this information electronically. The LBFP System can interface with multiple carriers and multiple financial institutions.

(53) There are at least four (4) possible outcomes from the application of the above procedure, namely, (1) unable to locate the cell phone (cell phone out or range, turned off, or other reason that the cell phone cannot be located), (2) able to locate the cell phone—the cell phone is not at home, work or other known location, (3) able to locate the cell phone—the cell phone is at home, work or other known location, the "known location" being the location, in addition to client's home address, where the client usually resides (i.e., work, family addresses), these locations are optional and normally would be entered by the client at registration (see registration process above for more details), (4) able to locate phone with a timestamp prior to the purchase/transaction time.

(54) With respect to each of the at least three (3) possible outcomes, a decision (score) table is created using at least the parameters: ΔD=distance between Location of Mobile phone and Location of Purchase Point, and ΔT=difference between Time located phone and Time of transaction, among potential parameters. The LBFP system may use additional factors to arrive at a final score/Fraud Confidence Level ("FCL"). These factors include a client's heading, speed, urban type/density, time of day, day of week, weather conditions, etc. As to ΔD, the time can range from 0 to 30 kilometers or more. As to ΔT, the time can range from 0 to 30 minutes or more. Depending upon the sensitivity desired for questioning whether a credit card purchase is valid, Fraud Confidence Level ("FCL") values are assigned within the LBFP System for each credit card transaction. When an FCL is calculated by the LBFP System to be above a threshold value, a flag will be raised as to a valid transaction. Alternatively, when an FCL is calculated by the LBFP System to be below a threshold value, a flag is raised as to a potentially fraudulent credit card use.

(55) For example, in the case of outcome (1), if the wireless provider is unable to locate the cell phone (no coverage, turned off, etc.), the LBFP System will switch into "search mode" as follows: (a) the system will keep attempting to locate the cell phone every 10 minutes for the next 30 minutes, or (b) if the location is determined within 30 minutes after the purchase transaction took place, the LBFP system will calculate the distance between the purchase location and the mobile phone location using an exemplar Table 1 to determine an FCL.

(56) TABLE-US-00001 TABLE 1 If the location of cell phone is within a distance (Km) of the The LBFP System tags purchase point and within 20 the transaction with an minutes of the transaction FCL of ½ 3 1 4 5 5 10 6 15 7 20 8 25 9 >30 10

(57) In the case of outcome (2)—if the LBFP System was able to locate the cell phone, though the cell phone is not at home, namely, the location of the cell phone was found within 10 minutes after the purchase transaction took place and the purchase type is physical (not online/internet), the LBFP System will calculate the distance between the purchase location or sale point and the mobile

phone location using an exemplar Table 2 to determine an FCL.

(58) TABLE-US-00002 TABLE 2 If the location of cell phone is within a distance (Km) of the purchase point and within 10 minutes of the The LBFP System tags the transaction transaction with an FCL of ½ 3 1 4 5 5 10 8 >10 10

(59) In the case of outcome (3)—the LBFP System will calculate the distance difference between the customer's known home, work or other known address and the location of the cell phone. If the LBFP System was able to locate the cell phone with the cell phone being at the above known locations, within 10 minutes after the purchase transaction took place AND the purchase type is online/internet, the LBFP System will calculate the distance between the above known locations and the mobile phone location using an example Table 3 to determine an FCL.

(60) TABLE-US-00003 TABLE 3 If the location of cell phone is within a distance (Km) of the The LBFP System purchase point and within 10 tags the transaction minutes of the transaction with an FCL of ½ 4 1 5 5 6 10 8 >10 19

(61) In the case of outcome (4)—a customer purchased goods or service from a physical location (e.g., store) and the LBFP System is unable to locate the cell phone. There may be situations whereby the wireless provider was able to acquire the customer's location prior to the purchase and store it in a temporary database. If the timestamp is close to the purchase time and the LBFP system is unable to get a newer location fix, then, in that case, the LBFP system may use the cached location information and ΔT to calculate the FCL using a scoring table similar to table 1. The cached location information can be either the location information stored on the location server or on the MT.

(62) In addition to the above data, the LBFP system may use additional factors in order to calculate the LFC/fraud score. These factors may be: time of day, day of the week, urban make (a suburb vs. downtown), weather conditions and traffic condition, among others. This is true for all possible scenarios.

(63) With respect to an online purchase, such as a purchase from the online company Amazon.com®, the LBFP System may either know in advance, or at the time of the purchase, the frequent or usual address of the purchaser, for instance, home, work or other known location. The configuration and customization can be defined both globally as a system-wide rule and on per individual basis when the subscriber registered for this service. Customization can include scoring/LFC threshold, known locations, and client notification methods (e.g., SMS, email).

(64) In the case of wireless network, GPS enabled cellular phones require, for the most part, a clear line of site with the sky in order to acquire GPS location. Since that does not always happen (in case the cellular phone is in the subway or other obstructed location), the location of the cellular phone sometimes does not match the exact location of the business. That is the reason the LBFP System compares both locations within a radius of X miles from such locations. (The number of X miles will be determined once an LBFP System in a particular environment has been through beta testing and becomes operational.) The X miles factor is also expected to vary in various geographical locations, such as rural locations versus large cities. Note also that there are cellular phones that can be located with means other than GPS. An example is the triangulation of the cellular phone's signals with surrounding cell towers. To the LBFP System, the manner by which the carrier obtains the mobile phone's location does not matter. The LBFP System will take into account parameters provided by the carrier such as heading, speed, acquisition-time and location error (accuracy).

(65) The invention has been described herein with reference to particular exemplary embodiments. Certain alterations and modifications may be apparent to those skilled in the art, without departing from the scope of the invention. The exemplary embodiments are meant to be illustrative, not limiting of the scope of the invention, which is defined by the appended claims.

Claims

1. A method for authenticating a transaction associated with a user's credit card number or debit card number, and further associated with the user's mobile phone, comprising, in order, the steps of: (A) verifying, prior to the transaction, an association between the mobile phone and the credit card number or debit card number, wherein verifying comprises: (i) receiving via the mobile phone at least the last four digits of the credit card number or debit card number, wherein the at least the last four digits have been input into the mobile phone; (ii) sending to the mobile phone a random number; and (iii) receiving via the mobile phone the random number; (B) receiving at least one of a calculated score and a calculated distance for the transaction, wherein the at least one of a calculated score and a calculated distance is based on at least: (i) a location of the mobile phone and a time associated with the location of the mobile phone, wherein the location of the mobile phone has been stored on the mobile phone and was determined via at least one of: GPS, Wi-Fi, antenna triangulation, and cellular base station ID; and (ii) the geographical proximity of the location of the mobile phone to a location associated with the transaction; and (C) generating a decision comprising at least one of: (i) allowing the transaction, (ii) sending an alert concerning the transaction, and (iii) preventing the transaction; wherein the transaction comprises at least one of an electronic purchase and a cash withdrawal, and the decision is based on the at least one of a calculated score and a calculated distance.
2. The method of claim 1, wherein the time associated with the location of the mobile phone is after the verification but before the transaction.
3. The method of claim 2, wherein the step of verifying further comprises receiving a confirmation that the at least the last four digits of the credit card number or debit card number are correct.
4. The method of claim 3, wherein the sending of the random number to the mobile phone utilizes SMS, and wherein the confirmation is performed by a bank or credit card company authorized to process the user's financial transactions.
5. The method of claim 2, wherein the sending of the random number to the mobile phone utilizes SMS.
6. The method of claim 1, wherein the step of verifying further comprises receiving a confirmation that the at least the last four digits of the credit card number or debit card number are correct.
7. The method of claim 6, wherein the sending of the random number to the mobile phone utilizes SMS, and wherein the confirmation is performed by a bank or credit card company authorized to process the user's financial transactions.
8. The method of claim 1, wherein the sending of the random number to the mobile phone utilizes SMS.
9. A method for authenticating a transaction associated with a user's credit card number or debit card number and further associated with a mobile phone, comprising, in order, the steps of: (A) verifying, prior to the transaction, an association between the mobile phone and the credit card number or debit card number, wherein verifying comprises: receiving, via the mobile phone, at least the last four digits of the credit card number or debit card number; sending, to the mobile phone, a random number; and receiving, via the mobile phone, the random number; and (B) generating a decision comprising at least one of: (i) allowing the transaction, (ii) sending an alert concerning the transaction, and (iii) preventing the transaction; wherein the transaction is at least one of an electronic purchase and a cash withdrawal; wherein the decision is based on at least one of a calculated score, a calculated travel speed, and a calculated distance for the transaction; wherein the at least one of a calculated score, a calculated travel speed, and a calculated distance is calculated based on at least the geographical proximity of a location of the mobile phone to a geographical location associated with the transaction; wherein the location of the mobile phone is determined via at least one of: GPS, Wi-Fi, antenna triangulation, and cellular base station ID; and

wherein the calculation of at least one of the calculated score and the calculated travel speed is further based on a time difference between a time associated with the transaction and a time associated with the location of the mobile phone, wherein the time associated with the location of the mobile phone is after the verification but before the transaction.

10. The method of claim 9, wherein the location of the mobile phone has been stored on the mobile phone, wherein the step of verifying further comprises receiving a confirmation that the at least the last four digits of the credit card number or debit card number are correct.

11. The method of claim 10, wherein the sending of the random number to the mobile phone utilizes SMS, and wherein the confirmation is performed by a bank or credit card company authorized to process the user's financial transactions.

12. The method of claim 9, wherein the location of the mobile phone has been stored on the mobile phone, wherein the sending of the random number to the mobile phone utilizes SMS.

13. A method for authenticating a transaction associated with a user's credit card number or debit card number, and further associated with a mobile phone, comprising the steps of: (A) verifying, prior to the transaction, an association between the mobile phone and the credit card number or the debit card number, wherein verifying comprises: receiving, via the mobile phone, at least the last four digits of the credit card number or debit card number, wherein the at least the last four digits have been input into the mobile phone; sending a random number to the mobile phone; and receiving the random number via the mobile phone; (B) receiving at least one of a calculated score, a calculated travel speed, and a calculated distance for the transaction; and (C) generating a decision based on the at least one of a calculated score, a calculated travel speed, and a calculated distance, the decision comprising at least one of: (i) allowing the transaction, (ii) sending an alert concerning the transaction, and (iii) preventing the transaction; wherein the at least one of a calculated score, a calculated travel speed, and a calculated distance is based on at least: (i) a location of the mobile phone and a time associated with the location of the mobile phone, wherein the location of the mobile phone was determined via at least one of: GPS, Wi-Fi, antenna triangulation, and cellular base station ID; and (ii) the geographical proximity of the location of the mobile phone to a geographical location associated with the transaction; wherein at least one of the calculated score and the calculated travel speed is further based on a time difference between a time associated with the transaction and the time associated with the location of the mobile phone.

14. The method of claim 13, wherein the location of the mobile phone has been stored on the mobile phone and wherein the time associated with the location of the mobile phone is after the verification but before the transaction.

15. The method of claim 14, wherein the step of verifying further comprises receiving a confirmation that the at least the last four digits of the credit card number or debit card number are correct.

16. The method of claim 15, wherein the sending of the random number to the mobile phone utilizes SMS, and wherein the confirmation is performed by a bank or credit card company authorized to process the user's financial transactions.

17. The method of claim 13, wherein the step of verifying further comprises receiving a confirmation that the at least the last four digits of the credit card number or debit card number are correct.

18. The method of claim 13, wherein the sending of the random number to the mobile phone utilizes SMS.