Journal of Finance and Investment Analysis, vol. 3, no.1, 2014, 51-67
ISSN: 2241-0998 (print version), 2241-0996(online)
Scienpress Ltd, 2014

Identity Management in the Retail Industry: The Ladder to Move to the Next Level in the Internet Economy

Ali M. Al-Khouri[1]

Abstract

Over the past decade, significant changes have been affecting the retail industry, largely due to the rapid pace of technological developments. With the advent of mobility and self-service models, retailers are aggressively working to stay ahead of the technology curve and meet new customers' demands and buying preferences. As such, retailers are seeking to be ubiquitous in today's digital world. However, being ubiquitous is still not enough. To better personalize and enhance service delivery, businesses need to know the users of their products and their service preferences. They also need to have the means through which identities can be ascertained. This article provides an overview of the main challenges facing the retail industry in this regard and some of the emerging realities of the Internet age that are impacting the industry. This paper argues that the insecurity of the Internet and the risk of identity theft are major obstacles to the development and optimal use of the Internet economy. The study aims to explore the role of modern identity management in the retail industry, while shedding light on one of the world's most renowned identity management infrastructures—in the United Arab Emirates (UAE)—and examining how reliable identity management systems can push the retail industry into new frontiers.

JEL classification numbers: L89
Keywords: Retailing, digital identity, identity management, national ID, e-economy**.**

1 Introduction

Today's business world is metamorphosing! The forces shaping our world are immense, complex, surprising, and challenging [1]. More than ever, the prosperity of organizations, societies, and individuals depends on the extent to which they can adapt to these forces and use them to their advantage (Ibid).

[1] Emirates Identity Authority, Abu Dhabi, United Arab Emirates and British Institute of Technology and Ecommerce, London, UK.

Article Info: *Received :* December 5, 2013. *Revised :* January 30, 2013.
Published online : March 1, 2014

Amid all this, the retail industry is in the throes of outgrowing conventional merchandising. The paradigm shift in consumer behavior from analogue to digital has not only affected the mode of sale but also the marketing modes and all other dimensions (see Figure 1). In fact, the Internet is increasingly influencing retail industry supply and demand [2]. Mobile technology, online marketing, and advanced distribution systems are fundamentally changing the nature of retailing (Ibid).

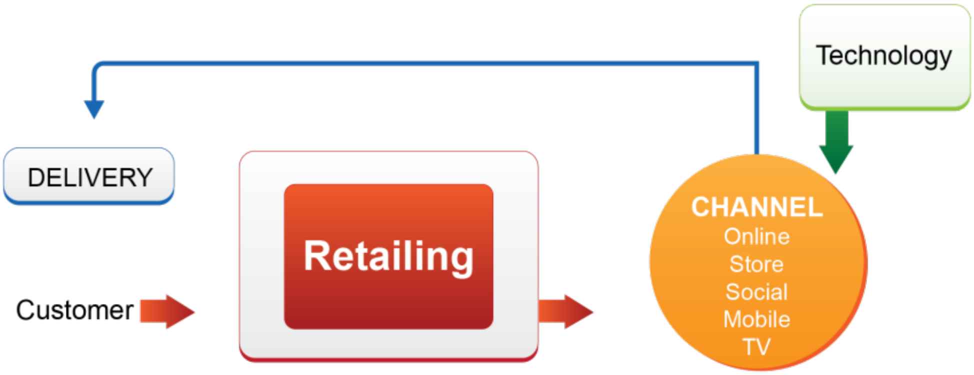


Figure 1: Technology’s impact on the retail industry

Studies indicate that more retailers are going global to capture a larger share of the $1.4 trillion e-commerce market [3]. The competition is obviously fierce and the marketplace is becoming more global and crowded. As such, retailers are constantly trying to find customers by cutting through the layers of value perception with their products and services aided by enhanced brand presence, which feeds the higher purchasing power of targeted customers.

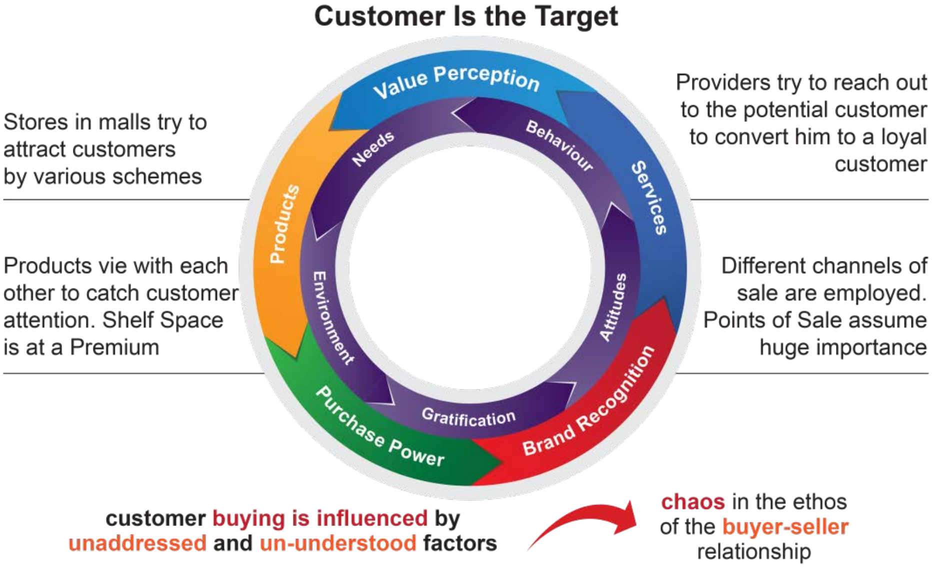

Customer Is the Target
Value Perception
Services
Brand Recognition
Purchase Power
Products
Needs
Behaviour
Attitudes
Gratification
Environment
Stores in malls try to attract customers by various schemes
Products vie with each other to catch customer attention. Shelf Space is at a Premium
Providers try to reach out to the potential customer to convert him to a loyal customer
Different channels of sale are employed. Points of Sale assume huge importance
customer buying is influenced by unaddressed and un-understood factors
chaos in the ethos of the buyer-seller relationship

Figure 2: Retail and marketing transformation

The impact of digitalization has been immense on everything related to a seller reaching the buyer and vice versa. The social networks have added a new dimension to the customers' online behavior. The paradox of human behavior today is such that people spend time more with their own selves while connected socially on the Internet. They spend time in the virtual presence of others but are in their own physical presence.

The mobility accorded by the smart phones and the availability of Internet across these devices has made people much more reclusive while being omni-present on social networks. Herein lies the paradox and the complexity of reaching out to the customer in terms of safely, security, and risk.

The level of trust in existing electronic identity management practices is not high enough for users to engage in more online transactions. Besides, identity systems in use are not sufficient to combat the globally growing crime of identity theft, which is wreaking havoc on economies worldwide. So why are markets not providing appropriate responses? How should governments approach this and what should be their role?

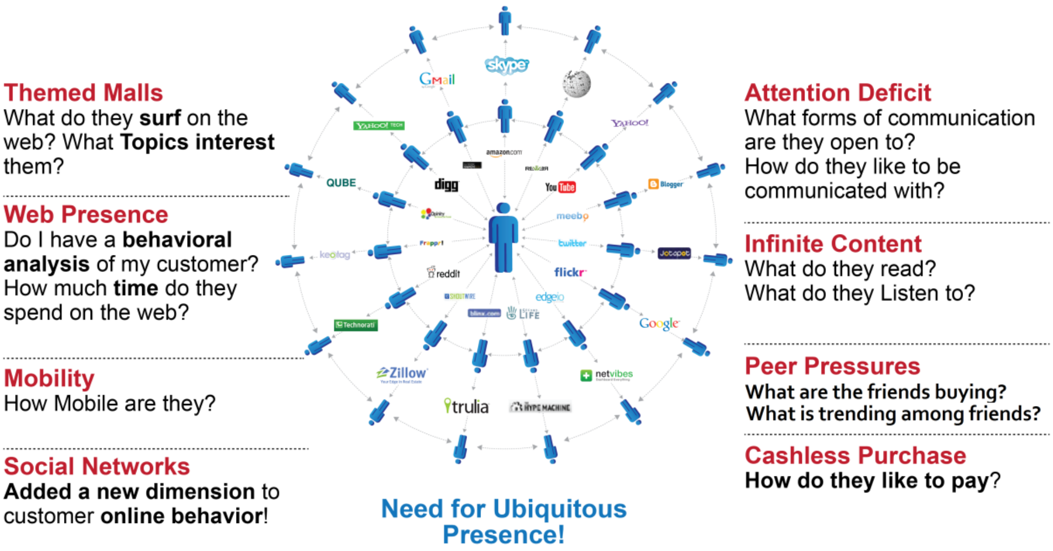
The objective of this article is to examine the role of modern identity management infrastructures in the revitalization of the online retail landscape and drive a positive transformation. We provide an overview of one of the leading and renowned government-owned identity management infrastructures that aims to reap the benefits of the Internet economy, namely the UAE national identity management infrastructure, which plays a significant role in pushing the retail industry into new frontiers.

The article is structured as follows. In section 2, we outline some of the challenges and emerging realities of the Internet age facing the retail industry. In section 3, we present some statistics around the mounting crime of identity theft and how it is impacting the growth of the retail industry. We examine the existing electronic identity management practices and why they are not sufficient to combat identity theft in the retail industry. In section 4, we provide an overview of the UAE's national identity management infrastructure and explain how the government aims to provide individuals, businesses, and government organizations with secure and reliable management of digital identity and personal data. The article concludes in section 5.

2 Changing Face of Retailing

In today's virtually driven world, the 7.1 billion population on Earth constitutes a potential customer base. From a retail perspective, knowing who among these are the most likely to buy particular products or consume particular services is a decisive set of data. It is clear that retailers have an opportunity to capture new customers online and increase sales through a compelling omni-channel strategy [4].

But how well do retailers know their customers in today's digital world? Global markets and innovative forms of multichannel retailing demand a fresh look at the dynamics of today's retailing environment [5]. Figure 3 depicts some emerging new realities of relationship management. Retailers need to understand these emerging consumer perceptions, especially in markets that are undergoing rapid change (Ibid).



Themed Malls
What do they **surf** on the web? What **Topics interest** them?

Web Presence
Do I have a **behavioral analysis** of my customer? How much **time** do they spend on the web?

Mobility
How Mobile are they?

Social Networks
Added a new dimension to customer **online behavior**!

Attention Deficit
What forms of communication are they open to?
How do they like to be communicated with?

Infinite Content
What do they read?
What do they Listen to?

Peer Pressures
What are the friends buying?
What is trending among friends?

Cashless Purchase
How do they like to pay?

Need for Ubiquitous Presence!

Figure 3: Emerging new realities of relationship management

Retailers around the world are under intense pressure to deliver services for customers that are personalized and integrated rather than adopt a one-size-fits-all approach. The transactional approach that multichannel retailers have traditionally applied to loyalty programs is no longer sufficient to build longer-term customer affinity [6,7]. The collision of the virtual and physical worlds is fundamentally changing consumers' purchasing behaviors [8]. Consumers are continuing to use the power of digital technologies to redefine the way in which they interact with retailers [6].

In essence, the realities of relationship management have changed. So one may wonder, how does this relationship get built? Collin Shaw [9] in *The DNA of Customer Experience* argues that customers are driven by a set of emotional values. Shaw's emotional values consist of a pyramid of four clusters as depicted in Figure 4.

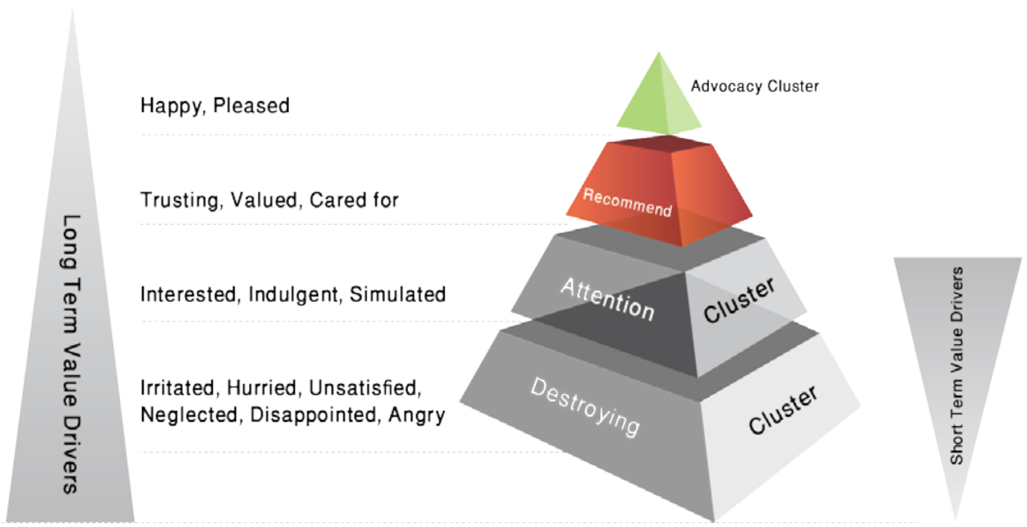

Long Term Value Drivers
Happy, Pleased
Trusting, Valued, Cared for
Interested, Indulgent, Simulated
Irritated, Hurried, Unsatisfied,
Neglected, Disappointed, Angry
Advocacy Cluster
Recommend
Attention
Cluster
Destroying
Cluster
Short Term Value Drivers

Figure 4: Hierarchy of emotional value**.** Source: Shaw [9]

The lowest cluster means that if businesses evoke these emotions with their customers, then they will lose value. This lower cluster represents the feelings when people are disappointed and frustrated towards a service or a product. The next cluster, “attention cluster,” is where the customers’ emotions are garnered to indulge in the beginning of an interest in a product/service. The positivity moves up by an enduring relationship of trust and value, with the customer being taken care of by the retailers. Here is where the relationship building takes place and where the retailer needs to know the customer more closely and personally. This is the most crucial part of a relationship-building exercise. Once the trust is gained, the customer becomes the advocate of the seller. But the unfortunate reality is that retailers today do not know their customers well—do they really know?

According to a survey released in January 2012 by Boston Retail Partners [10], 31% of North American retailers remain unable to identify their customers at the point of sale (POS). The survey also found that no retailer could identify customers connecting through mobile devices. As depicted in Figure 5, the most common customer contact information available includes telephone numbers (38%), customer/identification number (34%), email address (34%), name and address (31%), and member/club number (28%). But these still do not provide the reliable identification data that retailers need, as they might be subject to change from time to time.

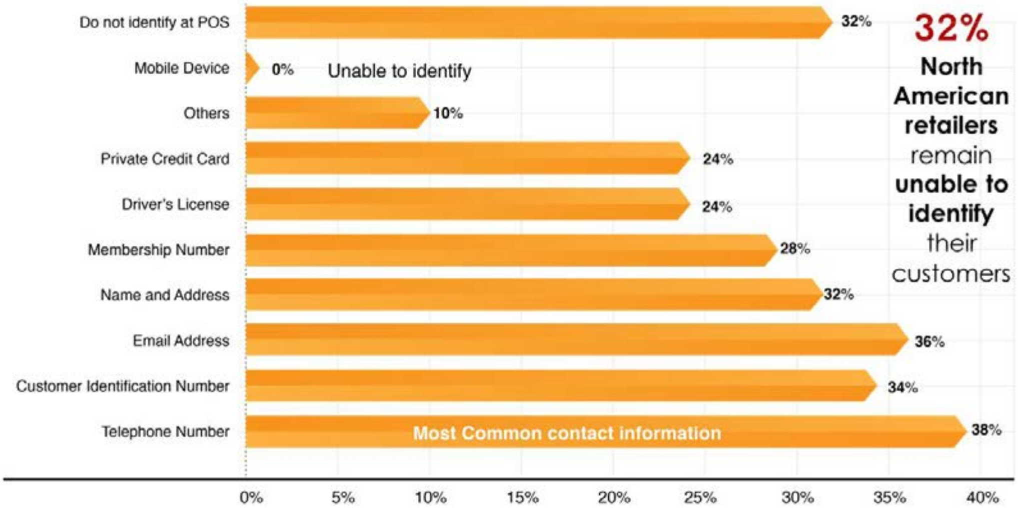


Figure 5: Boston Retail Partners Survey. Source: [9]

On the other hand, what makes this worse are the growing crimes related to identity theft, which has reached to a point where it is now threatening the growth of online retailers and the provisioning of financial and government services online as well. To shed light on the seriousness of this issue, the next section will provide some statistical elaboration.

3 Identity Theft

Retailers are turning to online systems to provide secure and easy-to-use transaction systems and to build deeper relationships with their now global customers. But such an online marketplace inspired newfangled risks for consumers and retailers [11]. For instance, online payment systems have created increasing demand for online customers to create and recreate identities with every retailer they interact with—all of whom are susceptible to different threats of identity theft (Ibid).

By definition, identity theft refers to the unauthorized use of an individual or entity's identity to conduct illicit activity [12]. Identity theft has increased at an alarming rate over the past few years [13]. Personal information lost in data breaches are frequently used to commit fraud [14]. While credit card numbers remain the most popular item revealed in a data breach, in reality, other information can be more useful to fraudsters (Ibid).

Data breaches represent a multifaceted threat. According to a study conducted by the Urban Institute's Justice Policy Center, identity theft and fraud will continue to be the fastest-growing crimes in the next five to 10 years; however, the nature of identity theft is likely to shift to more organized, high-stakes, global attacks [16]. The study also indicates that organized retail crime will continue to grow and become one of the most costly crimes experienced by the security industry (Ibid). As per the Javelin Strategy report, identity fraud incidents in 2012 increased by more than one million victims and fraudsters stole more than $21 billion—the highest amount since 2009 [16]. See Figure 6.

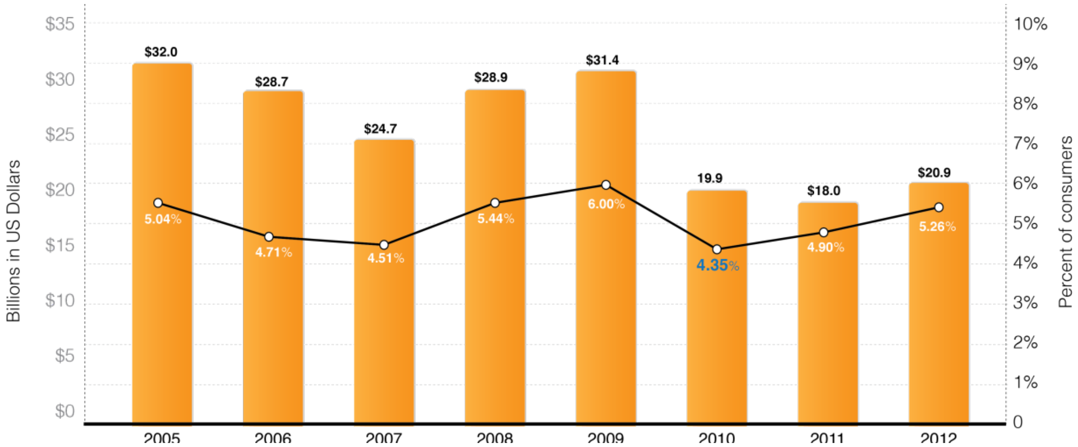


Figure 6: Overall identity fraud incidence rate and total fraud amount by year

In another study published recently by LexisNexis [17], data breaches continued to play a significant role in identity fraud, resulting in greater liability for merchants as the percentages of incidents increased from 12% in 2012 to 17% in 2013. In general, online-channel frauds increased by 36%, costing merchants $3.10 for each dollar of fraud losses. Not surprisingly, mobile merchants have incurred the greatest fraud losses as a percent of revenue among all merchant segments (0.75% in 2013). This is the only segment not to have benefitted from a decrease in fraud as a percent of revenue from 2012 to 2013. Mobile merchants are seeing an increase in revenue through this channel from 14% in 2012 to 19% in 2013. As depicted in Figure 7, Javelin report suggests that among all online users tablet owners have been the most susceptible to fraud; 80% more likely than all other consumers to become fraud victims.

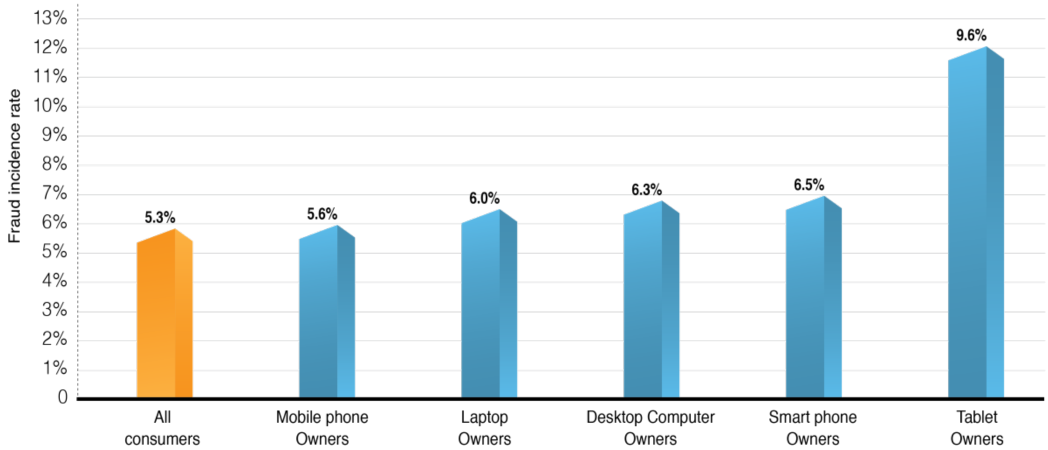


Figure 7: Fraud incidence by ownership of technology products. Source: [17]

Beyond a doubt, new technologies have been developed to contain identity-related frauds. Chip-and-pin (C&P) smart cards have been introduced in the banking industry to enable more secure payment systems for credit, debit, and ATM cards. But, it was found that the C&P and other remote payment fraud is on the rise in 2013, with the proportion of fraudulent transactions initiated online increasing by 36%, and those initiated by mail or telephone doubling in the same time period.

The opportunity and anonymity that are touted as the secure features make the C&P and other types of remote payment fraud appealing to fraudsters. Many means exist today to glean and misuse user payment information and account credentials. However, the fact that fraudsters are exploiting the online channel does not mean that they are abandoning the physical channel just yet. Merchants with a physical presence saw an increase in the proportion of fraud through the physical channel as well (Figure 8).

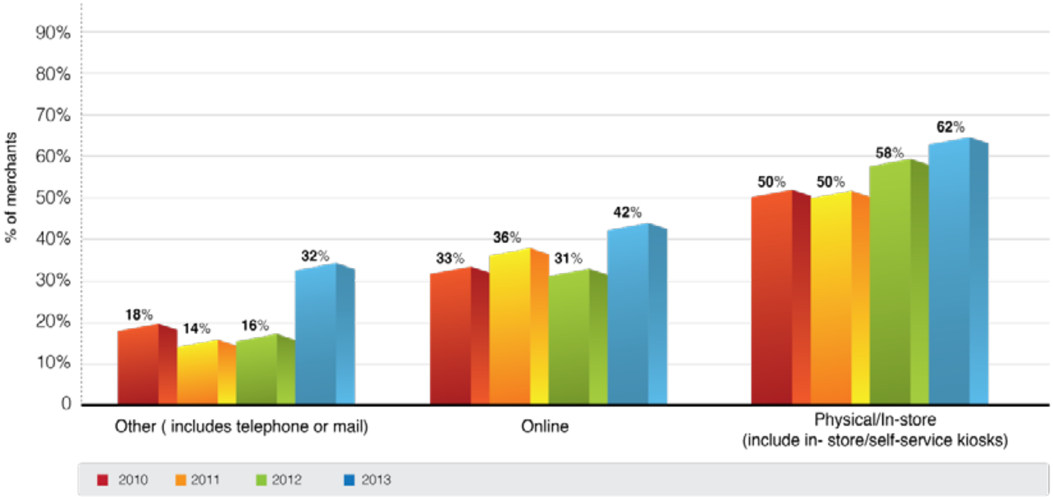


Figure 8: Percentage of fraudulent transactions attributable to channels among merchants. Source: LexisNexis [17]

Lost and stolen merchandise is declining as a percentage of fraud losses. Therefore, identity theft (involving fraudulent card, check, or mobile payments), and, to a lesser extent, fraudulent requests for return and refund, are likely driving the increase in the proportion of physical channel fraudulent transactions in all fraud. Proper authentication at the POS will help merchants avoid the charge-backs and fees to financial institutions that may result from identity fraud. Improving company policies designed to limit fraudulent returns and refunds may be a difficult balancing act for customer-service-focused merchants, but they may help to curtail the not-inconsequential 18% of fraud losses resulting from this type of fraud.

Going further on these reports, the merchant community is in general agreement with the existence of fraud owing to identity theft. The majority seems to have accepted this as a risk that is inevitable, but current risk mitigation mechanisms seem to do little to thwart these fraudulent activities (Figure 9).

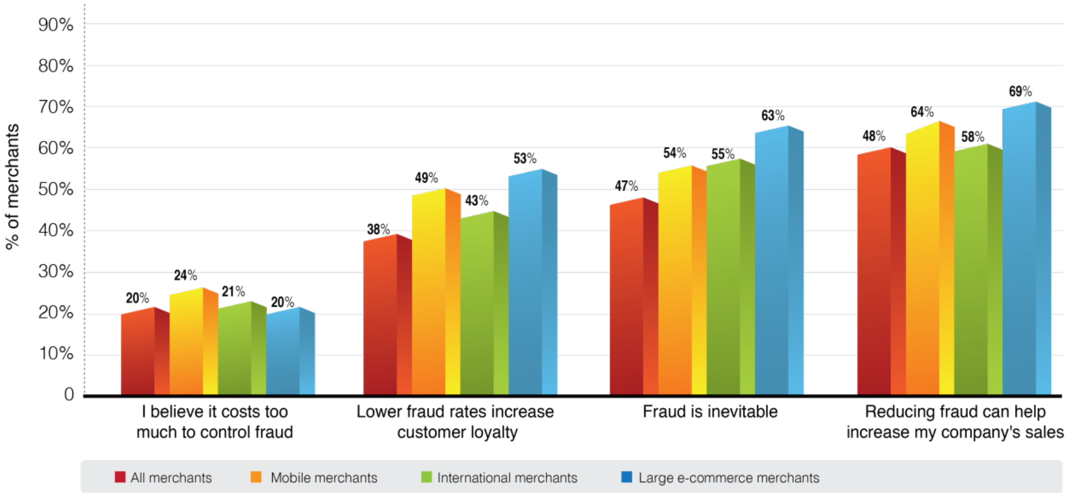


Figure 9: Merchants' attitude towards e-commerce fraud. Source: LexisNexis [17]

The message to note here is that, while the community accepts risks due to identity frauds as inevitable and might even consider them for defining their risk appetite, the loss of opportunity due to perceived threats is huge. Customers who find that there are little or no efforts in thwarting identity theft from the retailers are less likely to do business with them. The largest sector of the retail, the small and medium establishments, thus stand to lose and lose heavily.

As depicted in Figure 10, the biggest challenge to address is in the verification of customers' identities. Thirty-nine percent of merchants consider verifying customers' identity to be the most challenging aspect of selling to consumers at the point of sale and remotely.

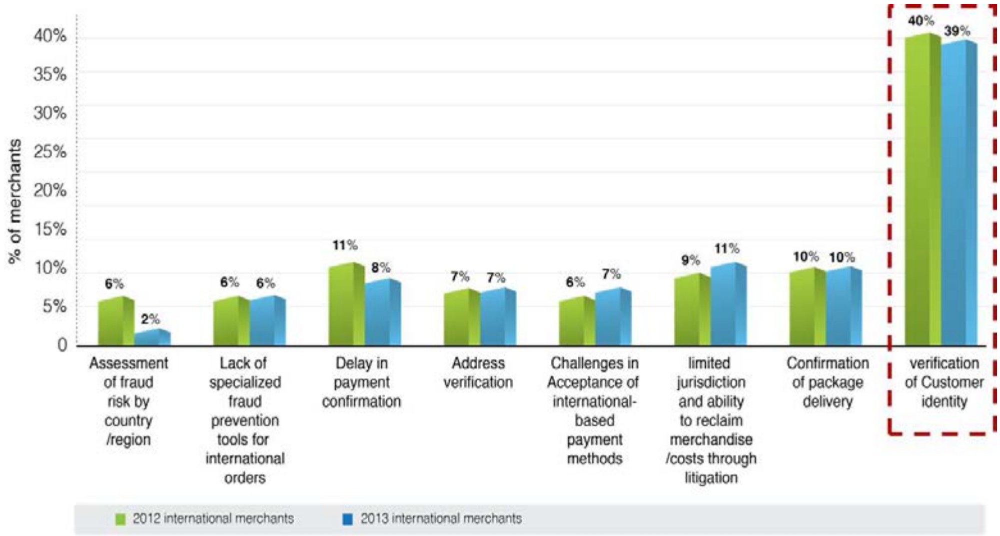


Figure 10: Top challenges in controlling international fraud (2012–2013).
Source: LexisNexis [17]

The issue requires a more comprehensive approach to protecting personal information [18, 19]. The ad hoc way in which online identities are managed today cannot withstand the increasing assaults from expert criminal attackers [17]. A new approach to securely managing online identity is essential—namely, a system that uses an interoperable, vendor-neutral framework and gives end users more direct control over their digital identity (Ibid).

To unlock the full value potential, the retail industry needs to embrace a new paradigm for digital identity applications. According to a report by the Boston Consulting Group, the value created through digital identities could reach 1 trillion euros in Europe by 2020 [10]. Two-thirds of digital identity's total value potential stands to be lost if stakeholders fail to establish a trusted flow of personal data (Ibid).

Faced with such business opportunities, governments around the world have initiated national identity management infrastructure development programs to leverage strong identity credentials in electronic environments for both public and private sectors use. The next section provides an overview of one of the most renowned and ambitious initiatives in the world that aims to provide individuals, businesses, and government organizations with secure and reliable management of digital identity and personal data.

4 Government-Owned Digital Identity Management to Support e-Economy Development

The government of the UAE initiated a national identity management infrastructure development program in 2003. All citizens and legal residents were enrolled in 2012. The enrollment process consisted of capturing the biometrics of all those above the ages of 15, mainly fingerprints and facial recognition supplemented now by iris recognition, and issuing them in a digital format as the national identification in the form of a unique permanent number and smart card.

The national identity management infrastructure in the UAE is based on a key public infrastructure, which is a cryptographic technique that enables users to securely communicate on an insecure public network and reliably verify the identity of a user via digital signatures [21].

As depicted in Figure 11, the UAE smart card provides advanced user authentication capabilities more securely than standard usernames and passwords in addition to electronic signature capabilities to sign documents to ensure non-repudiation. The card also enables establishing a person's identity on-site or remotely, allowing secure and trusted transactions. The multi-factor authentication provides match-on-card and match-off-card features facilitates validation, verification, and authentication of an identity. The card holder then gets all of the identity-based services.

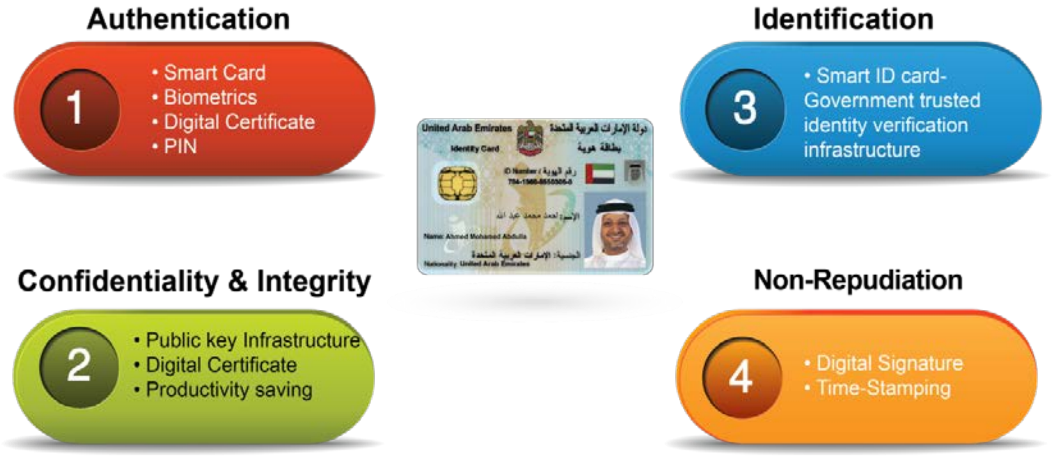


Figure 11: UAE national ID card advanced capabilities

The UAE has recently set up an online national validation gateway to provide online card holder authentication, verification, and validation services to public and private sector organizations. The UAE national validation gateway's strong authentication services offer the widest array of authentication choices to meet the needs of public and private organizations. In principle, the use of the national gateway provides more secure, online, real-time validation, verification, and authentication of identity credentials (i.e., card, transaction, and holder genuineness; see also Figure 12).

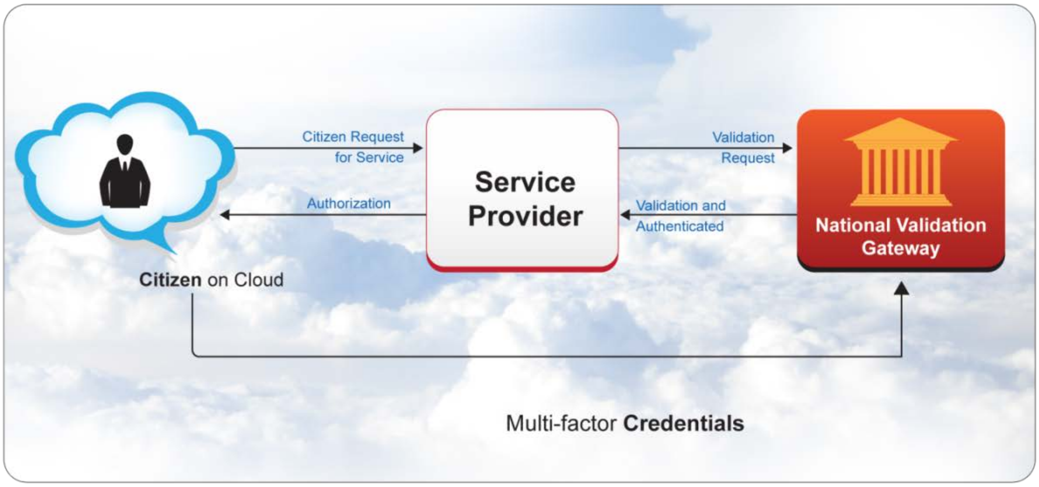


Figure 12: Online validation gateway scenario

The national validation gateway ensures that not only are identification processes made seamless to enhance service delivery but they also vastly improve business processes, leading to strong bottom lines (Figure 13). Prevention of identity theft leads to direct prevention of losses and contributes to growth in over-the-counter sales and online. Increased online sales directly implies a lower cost of sales and higher margins.

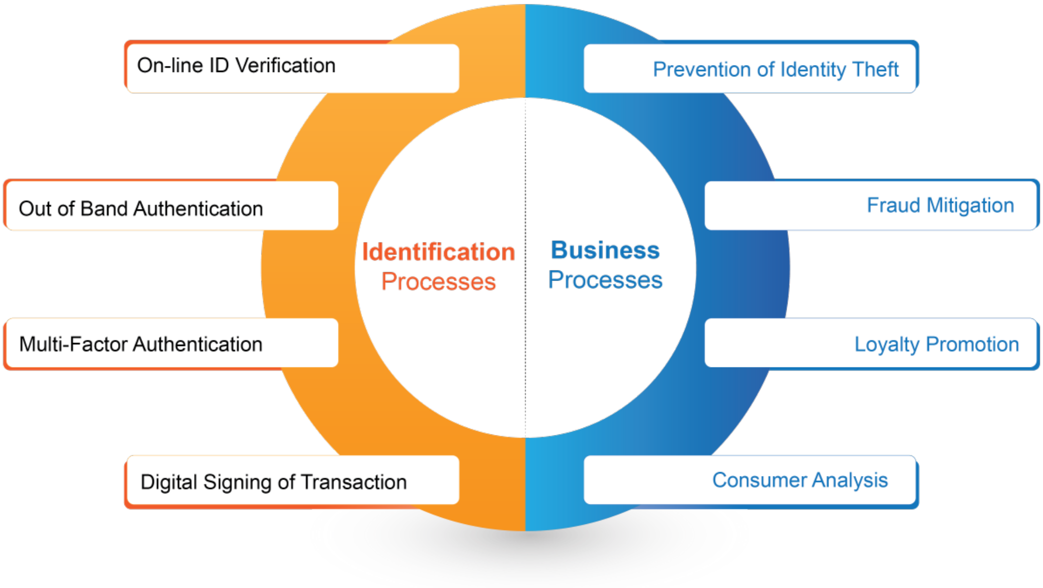


Figure 13: National validation gateway impact
on identification and business processes

A recent study conducted by Ernst & Young for the UAE government reported that across different sectors in UAE, while the customer is "registered," the business still asks for identification to be provided, but during the transactions a sizeable number of companies do not identify their customers securely. More importantly, for any identification need, the customer has to visit the service provider's premises (Figure 14). Moreover, this process is completely lacking in the retail industry. The study suggests that remote transactions are not secure enough due to lack of proper identity verification in the retail industry in the UAE.

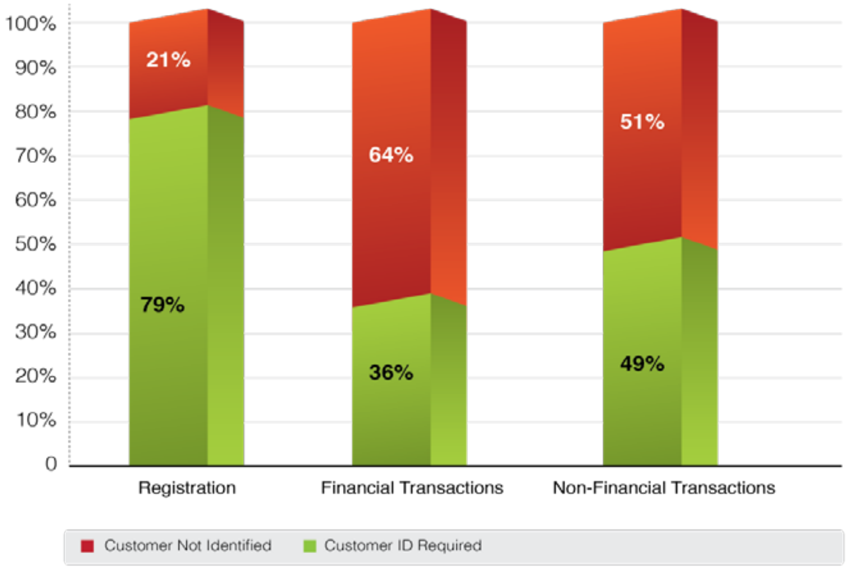


Figure 14: Survey results of ID verification in UAE

The study also suggested that potential benefits to the UAE economy could exceed a trillion dollars in local currency ($271 billion) in terms of productivity enhancement, direct consumer benefits, reduction in space utilization, paper reduction (contributing to a green environment), and cost savings from diverse other aspects (Figure 15).

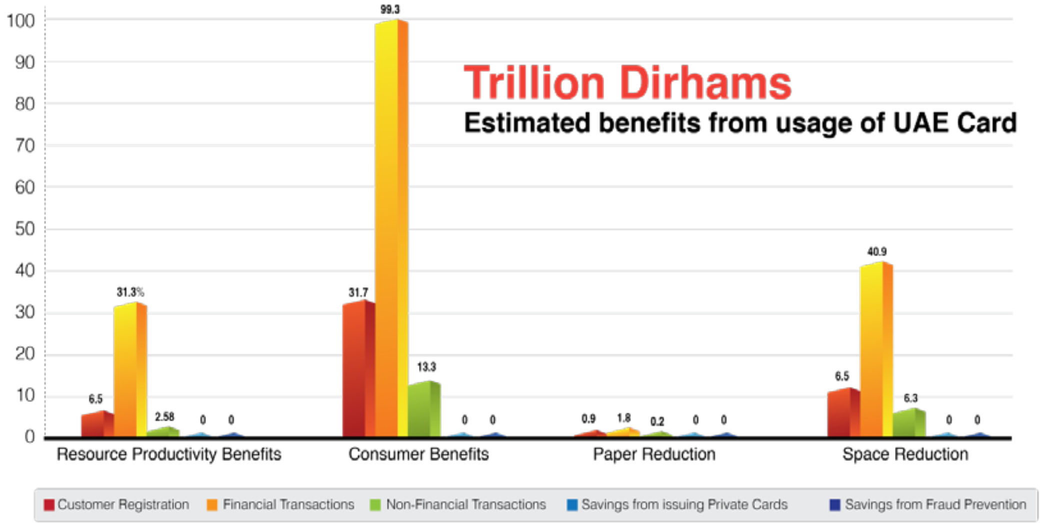


Figure 15: Identity management infrastructure potential benefits to UAE economy

The UAE identity management infrastructure offers significant opportunities for retailers. It provides the needed support to guide the public sector and businesses for setting efficient framework conditions for innovation across the public and private sectors while enhancing security, privacy, and trust in the Internet economy. The UAE government is also working on extending and leveraging its existing national identity management infrastructure to support the authentication of smart phone and mobile device users as well [21]. Retailers will have the same credentials available for verification in such mobile environments and significant opportunities that may exceed current potential value reported above.

5 Concluding Remarks

Solid identity management and strong credentialing practices enable the verification of identities that are critical for the retail industry. In fact, identity management is the main vehicle for building sustainable economies. As a key instrument for establishing the identity, the UAE national identity card system provides a strong framework for increasing the governance and providing internal controls. The card and the identity management comply with all international standards and regulations and provide a secure verifiable identity for individuals. The outcome is the ability to have self-service interfaces that enable a reduction in costs for the services using automation for policy enforcement. This ability, backed by a centralized audit trail, provides a strong backbone for businesses to be carried out innovatively. This not only reduces IT operational costs but also provides the much-touted user efficiency and productivity (Figure 16).

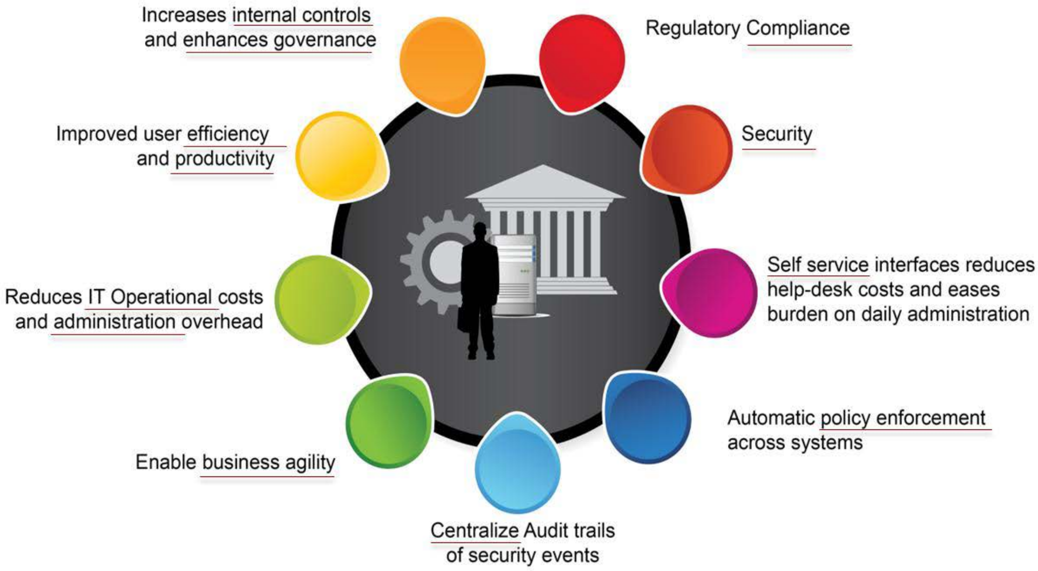

Increases internal controls and enhances governance
Regulatory Compliance
Improved user efficiency and productivity
Security
Self service interfaces reduces help-desk costs and eases burden on daily administration
Reduces IT Operational costs and administration overhead
Automatic policy enforcement across systems
Enable business agility
Centralize Audit trails of security events

Figure 16: Identity management contribution dimensions

Adopting solutions designed to capitalize on national identity management infrastructure allows businesses to navigate the shifting retail landscape and drive positive transformation, including critical objectives such as the delivering a smarter shopping experience and building smarter merchandising and supply networks. These advanced technologies provided by government have staggering capabilities to revitalize the retail industry. The applications built on the use of digital identity can drive massive value growth for both public and private sector organizations [10]. For retailers and online businesses, such an infrastructure has value potential to improve process automation, user enablement, personalization, enhanced delivery, personal data-driven R&D, and secondary monetization (Ibid). Government-owned identity management infrastructures are essential building blocks for the Internet to operate as a platform for economic development and social progress.

Different countries have taken different approaches. The approach followed by the government of the UAE is based on its leadership vision that governments' involvement is needed to succeed in the digital economy. This is to ensure ready and affordable access, a level playing field, and an open competitive environment that enables everyone to tap the economic benefit of the Internet [3]. Governments need to intervene if they want to be winners. They should aim to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce (Ibid).

References

[1] I. Pearson, Business Redefined, Ernst & Young, (2010), [Online] Available from: http://www.ey.com/Publication/vwLUAssets/BusinessRedefined-FINAL/$FILE/BusinessRedefined-FINAL.pdf (October 11, 2013).

[2] R. Levis, The Impact of the Internet on Retail Property. Aviva Investors, (2013), [Online] Available from: http://www.avivainvestors.co.uk/pension_schemes/internet/groups/internet/documents/salessupportmaterial/pdf_029761.pdf (October 13, 2013).

[3] D. Dean, S. Digrande, D. Field, A. Lundmark, J. O'Day, J. Pineda, and P. Zwillenberg, The Connected World: The $4.2 Trillion Opportunity - The Internet Economy in the G-20, The Boston Consulting Group, (2012), [Online] Available from: https://publicaffairs.linx.net/news/wp-content/uploads/2012/03/bcg_4trillion_opportunity.pdf (November 22, 2013).

[4] WalkerSands, Reinventing Retail: What Businesses Need to Know for 2014, (2013), [Online] Available from: http://www.walkersands.com/pdf/Walker-Sands-Future-of-Retail-Whitepaper.pdf (October 11, 2013).

[5] C. Kaufman-Scarborough, and S. Forsythe, Current issues in retailing: Relationships and emerging opportunities, *Journal of Business Research*, **62**, (2009), 517–520.

[6] M. Burt, J. Davison, R. Hetu, and K. Welch, Predicts 2014: Digitalization in Retail Means M-Commerce Grows, E-Commerce Slows, Personalization Misfires and 3D Printing Transforms, Gartner, (2013), [Online] Available from: https://www.gartner.com/doc/2625216 (November 12, 2013).

[7] K. Welch, Excellent Execution of Customer Basics Is Key to Building Loyalty. Gartner, (2013), [Online] Available from: https://www.gartner.com/doc/2631834 (October 11, 2013).

[8] Deloitte, Global Powers of Retailing 2013 Retail Beyond. Deloitte, (2013) [Online] Available from: http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Industries/Consumer%20business/Deloitte_Global_Powers_of_Retail_2013.pdf (November 12, 2013).

[9] C. Shaw, The DNA of Customer Experience: How Emotions Drive Value, Palgrave Macmillan, New York, (2007).

[10] Liberty Global, The Value of our Digital Identity, Boston Consulting Group, (2012), [Online] Available from: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (October 15, 2013).

[11] S. Lachut, The Future of Retail 2014. A PSFK Report. PSFK LABS, (2013), [Online] Available from: http://www.psfk.com/publishing/future-of-retail-2014 (October 11, 2013).

[12] J. Craig, J. Kerben, J.D. King, E.T. Lanoue, K. Lissy, C. Sailer, K. Schwomeyer, J. Thomas, and B. Yellen, The Current and Future Landscape of Identity Theft, (2013), [Online] Available from: http://blog.thomsonreuters.com/wp-content/uploads/2013/11/IDT-WhitePaper-final-20131030-2.pdf (November 18, 2013).

[13] R. Cantor, Identity Theft, Destiny Image, USA, (2013).

[14] ITAC, Research and Statistics. Identity Theft Assistance Center, (2013), [Online] Available from: http://www.identitytheftassistance.org/pageview.php?cateid=47 (November 22, 2013).

[15] La Vigne, N.G., Hetrick, S.S. and Palmer, T., The Urban Institute, (2008), [Online] Available from: http://www.urban.org/UploadedPDF/411758_crime_trends.pdf (October 11, 2013).

[16] Javelin Strategy and Research, How Consumers can Protect against Identity Fraudsters in 2013, (2013), [Online] Available from: https://www.javelinstrategy.com/uploads/web_brochure/1303.R_2013IdentityFraudConsumerReport.pdf (October 11, 2013).

[17] LexisNexis, True Cost of Fraud Study: Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud, (2013), [Online] Available from: http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf (October 15, 2013).

[18] A.M. Al-Khouri, PKI in Government Digital Identity Management Systems, *European Journal of ePractice*, **4**, (2012a), 4-21.

[19] A.M. Al-Khouri, An Innovative Approach for e-Government Transformation, *International Journal of Managing Value and Supply Chains,* **2**(1), (2011), 22-43.

[20] Microsoft, Online Identity Theft: Changing the Game – Protecting Personal Information on the Internet. Microsoft Corp. USA, (2012), [Online] Available from: http://www.telecomasia.net/content/online-identity-theft-changing-game (October 11, 2013).

[21] A. Carlisle, and L., Steve, *Understanding PKI: concepts, standards, and deployment considerations,* Addison-Wesley Professional, (2003), 11–15.

[22] A.M. Al-Khouri, Identity and Mobility, Proceedings of Electronic Government Megatrends Conference, 2013 Cartes Exhibition, November 19-21, Paris, France.

[23] A.M. Al-Khouri, Emerging Markets and Digital Economy: Building Trust in the Virtual World, *International Journal of Innovation in the Digital Economy*, **3**(2), (2012b), 57-69.

[24] A.M. Al-Khouri, eGovernment Strategies: The Case of the United Arab Emirates, *European Journal of ePractice*, **17**, (2012c), 126-150.

[25] N. Baird, and W. Raj, Customer-Centricity Drives Successful Omni-Channel Retailing: Insights from a webinar presented by Retail Systems Research (RSR) and SAS. SAS Institute Inc. (2012), [Online] Available from: http://www.storeconference.ca/sites/default/files/docs/ecobag/SAS.pdf (October 10, 2013).

[26] M.T. Banday, and J.A. Qadri, Phishing - A Growing Threat to E-Commerce, *The Business Review*, **12**(2), (2007), 76-83.

[27] A. Brust, Five Big Data Trends Revolutionizing Retail, (2013), [Online] Available from: http://www.zdnet.com/five-big-data-trends-revolutionizing-retail-7000019510/ (October 10, 2013).

[28] L. Costa, and F. Fernandes, Successful Retail Innovation in Emerging Markets: Latin American Companies Translate Smart Ideas Into Profitable Businesses. Booz & Company, (2006), [Online] Available from: http://www.booz.com/media/file/SuccessfulRetailInnovationinEmergingMarkets.pdf (November 12, 2013).

[29] T.H. Davenport, and j. Dyché, Big Data in Big Companies. SAS Institute Inc, (2013), [Online] Available from: http://www.sas.com/content/dam/SAS/it_it/doc/whitepaper2/big-data-big-companies-2282455.pdf (November 18, 2013).

[30] M. Graham, Big data and the end of theory?, The Guardian, (2012), [Online] Available from: http://www.theguardian.com/news/datablog/2012/mar/09/big-data-theory (November 18, 2013).

[31] Gupta, Yuvika, When BI Meets CRM: An Emerging Concept in Retail Industry (July 16, 2013). Publishing India Group, [Online] Available from: http://ssrn.com/abstract=2294468 (November 18, 2013).

[32] S. LaValle, E. Lesser, R. Shockley, M.S. Hopkins, and N. Kruschwitz, Big Data, Analystics and the Path from Insights to Value. MIT Sloan Management Review. 52(2), (2011), 21-31. http://www.ibm.com/smarterplanet/global/files/in_idea_smarter_computing_to_big-data-analytics_and_path_from_insights-to-value.pdf (October 11, 2013).

[33] M. Lips, Rethinking citizen - government relationships in the age of digital identity: Insights from research. Journal of Information Polity, **15**(4), (2010), 273-289. http://www.victoria.ac.nz/sog/researchcentres/egovt/publications/rethinking_citizen_govt.pdf

[34] OECD, National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing, (2011), http://dx.doi.org/10.1787/5kgdzvn5rfs2-en (December 1, 2013).

[35] P. Ohm, Don't Build a Database of Ruin, Harvard Business Review, (2012), [Online] Available from: http://blogs.hbr.org/2012/08/dont-build-a-database-of-ruin/ (October 11, 2013).

[36] S. Shah, A. Horne, and J. Capellá, Good Data Won't Guarantee Good Decisions, Harvard Business Review, (2012), [Online] Available from: http://hbr.org/2012/04/good-data-wont-guarantee-good-decisions/ar/1 (October 17, 2013).

[37] R.G. Smith, Does economic crime really matter in the world of today? Public and business perceptions in Australia. Cambridge Symposium on Economic Crime, (2013), [Online] Available from: http://www.aic.gov.au/media_library/conferences/other/smith_russell/2013-09-cambridge.pdf (October 11, 2013).

[38] C. Snijders, U. Matzat, and U.D. Reips, Big Data: Big gaps of knowledge in the field of Internet, *International Journal of Internet Science*, **7**, (2012), 1-5. http://www.ijis.net/ijis7_1/ijis7_1_editorial.html (October 11, 2013).