Chapter V

Identity Theft and E-Fraud Driving CRM Information Exchanges

Alan D. Smith, Robert Morris University, USA

Allen R. Lias, Robert Morris University, USA

Abstract

Fraud and identity theft have been increasing with the use of e-commerce. In the U.S. alone, it has been estimated that victims may spend on average $1,500 in out-of-pocket expenses and an average of 175 hours in order to resolve the many problems caused by such identity thieves. Organizations that engage in e-commerce as a large part of their business need to protect their customers against these crimes. An empirical study of 75 managerial employees and/or knowledge workers in five large organizations in Pittsburgh, PA, revealed a number of interesting concepts of find out how much information they share with others, what the likelihood is that they will conduct business online, and whether or not they take steps to protect their personal identity and credit. Model construction and implications were generated concerning steps that employees and customers may take to avoid identity theft.
Introduction

Consumer Relationship Management (CRM) Basics

The Web has created a world of convenience for consumers who wish to purchase or gather information about a product, but online technology and e-businesses pose as many threats as opportunities. The concern by consumers about their private information is an ongoing headache, for example, a recent search on Google for the key words “identity theft” about 79,500,000 items. Many issues by consumers have been associated with the possibility that their information could be used or stolen by cyber-criminals and abused before the consumer could find out. Several studies have been produced that show the perceptions of consumer risk and how they may be the main complication in online e-commerce in the future (Culnan, 1999; Fernandez & Miyazaki, 2001). For this reason, it is important to provide security and privacy for online users in e-business and e-commerce (Smith, 2005a, 2005b, 2005c). With security and privacy also comes the question of how much is needed?

Organizations of every conceivable size and description are automating the way they do business in order to cut costs, speed service, and reach customers, suppliers and partners more easily and in a more efficient manner. As a result of these trends associated with e-commerce, more consumer and business data are online to meet the requirements of e-commerce. Throughout much of the academic and practitioner literature, trust, privacy of information, and systems security (Drake, 2003; Smith, 2002; Smith & Rupp, 2002a, 2002b) are important reoccurring themes factors in customer retention for a firm that engages in e-commerce. For example, research by Visa USA, which helped to develop the CyberSource fraud prevention software, credit card fraud on the Web is three times as likely as it is for all other forms of card use (Smith, 2002). In addition, Smith (2002) suggested, “Addressing customer service issues are extremely critical for the firm’s continued survival and long-term success, but these services are merely academic if the firm ignores to enhance customer loyalty and retention through the development of trust” (p. 156). Hence, to promote trust and confidence, managers of Web sites should educate customers about the company, its products, its security and privacy policies, and prices. Failure of an e-commerce firm to instill a sense of security and have the appropriate technology and software to actually protect personal and proprietary information will most certainly lead to customer attrition and destruction of sound customer relationship management (CRM) principles.

Since several CRM-based studies have shown that it is more expensive to continually attract new customers than it is to satisfy existing, loyal customers, the cost of customer attrition can be financially draining on an e-commerce firm. In addition, the age of e-business decreases a customer’s switching costs as a competitor’s product or service is just a mouse-click away (Anton & Petouhoff, 2002). In consideration
Related Content

Designing a New Integrated IT Governance and IT Management Framework Based on Both Scientific and Practitioner Viewpoint
[www.igi-global.com/article/designing-new-integrated-governance-management/74371?camid=4v1a](www.igi-global.com/article/designing-new-integrated-governance-management/74371?camid=4v1a)

The Syngenta Architecture Story
[www.igi-global.com/chapter/syngenta-architecture-story/19434?camid=4v1a](www.igi-global.com/chapter/syngenta-architecture-story/19434?camid=4v1a)

Linking the Impact of IT Investments to Productivity and Profitability
[www.igi-global.com/article/linking-impact-investments-productivity-profitability/53843?camid=4v1a](www.igi-global.com/article/linking-impact-investments-productivity-profitability/53843?camid=4v1a)
RFID Implementation in Australian Hospitals: Implications for ICT Sector and Health Informatics
www.igi-global.com/article/rfid-implementation-in-australian-hospitals/112077?camid=4v1a