Identity Theft and E-Fraud as Critical CRM Concerns

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, Pennsylvania, revealed a number of interesting facts about 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.

Keywords: CRM; e-commerce; e-fraud; e-security; empirical studies; identity theft; knowledge workers; models

INTRODUCTION

Consumer Relationship Management (CRM) Basics

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 theme 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, revealed that credit card fraud on the Web is three times as likely as it is for all other forms of card use (Smith, 2002). In addi-
tion, 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 of these concepts, customers who do not feel that their personal and financial information will be protected need only to inspect the next Web site for a firm that is able to meet their needs. The exponential increase in the occurrence of identity theft makes this assurance more important than ever, for both e-commerce firms and their customers.

**Sources of Identity Theft**

A major type of identity theft occurs when another person uses the chosen victim’s personal information to open fraudulent accounts. Personal information includes, but is not limited to, name, address, driver’s license, social security number (SSN), telephone number, mother’s maiden name, bank accounts, and credit card numbers. The resulting incurred expenses often remain unknown to the victim until he/she applies for some type of credit and is subsequently denied. The reason these unauthorized charges remain unknown is because thieves typically divert the statements to another billing address. The advantage of the Internet for thieves for leveraging tools for illegal activities is that it provides worldwide accessibility, allowing them to transmit and collect information globally. Thieves may do this by using e-mails to lure victims to freely give information (as in the recent sham concerning verifying credit card information for continued use of Paypal) and/or by obtaining information found by hacking into personal files.

Today’s thieves have many avenues in which to steal individual identities. While the rise in the crime rate corresponds with the growth of the Internet, less than 1% of identity theft cases can be linked to Internet usage. This may be due to a lack of ability to track the source of theft back to the Internet. Old-fashioned thievery is still the most prevalent means of stealing identities. For example, simple “dumpster diving” and “shoulder surfing” are identity theft’s number one partner in crime. Dumpster diving occurs when thieves sift through trash to find statements or solicitations that unsuspecting individuals failed to tear up. Shoulder surfing is the term used when a thief literally look over someone’s shoulder to obtain information.

Another widely used method of obtaining information is “credit-card skimming.” Through enlisting the help of restaurant personal, for example, a criminal can attach a skimmer to your credit card. Typically, a skimmer is about the size of a credit card and it collects your credit card...
Related Content

Adaptation of the UML to Formalized Software Development Process Assessment and Modeling- Dedicated Metamodel and Case Study
[www.irma-international.org/chapter/adaptation-uml-formalized-software-development/18404/](www.irma-international.org/chapter/adaptation-uml-formalized-software-development/18404/)

Digital Forensics
[www.irma-international.org/chapter/digital-forensics/18396/](www.irma-international.org/chapter/digital-forensics/18396/)

A Framework for Interfacing Unstructured Data Into Business Process From Enterprise Social Networks

Factors Influencing Users' Intention to Continue Using ERP Systems
[www.irma-international.org/chapter/factors-influencing-users-intention-continue/43387/](www.irma-international.org/chapter/factors-influencing-users-intention-continue/43387/)

The Underlying Test: Human, Organisational and Technical Considerations adjoined with Critical Success Factors when implementing ERP: A Cases study of a UK SME
[www.irma-international.org/chapter/underlying-test-human-organisational-technical/41824/](www.irma-international.org/chapter/underlying-test-human-organisational-technical/41824/)