Online Security Cues and E-Payment Continuance Intention

Echo Huang, National Kaohsiung First University of Science and Technology, Taiwan
Fa-Chang Cheng, National Kaohsiung First University of Science and Technology, Taiwan

ABSTRACT

Previous studies consider confidence in the Internet as a means of payment and existence of a legal framework that protect consumers in their activities on the Internet are the critical issues of B2C success. To respond, this study extends the IS Continuance Model with Cue Utilization Theory to examine the impact of offering e-payments to online users, specifically, the relationship between their perceived benefits, legal protection, risk avoidance, and satisfaction with prior experiences. The analytical results presented in this study indicate that perceived cues (benefits, legal protection and risk allocation) differentially affect consumer behavior. Notably, perceived cues and confirmation associated with satisfaction have influences on e-payment continuance intention. That is, if consumers’ perception of online security cues increases, their intentions to continue use of e-payment increase even if the systems or services are perceived low reliability. Finally the practical and theoretical implications of this study are discussed.

Keywords: B2C, E-Payment, Perceived Benefits, Perceived Legal Protection, Perceived Risk

INTRODUCTION

The success of electronic commerce depends upon effective e-payment systems. Accompanying the exponentially rapidly growth of the Internet and online business, more and more innovative Internet payment methods have been developed to address the needs for greater speed and convenience (Leclerc et al., 1995). An electronic payment is defined as a payment services that utilize information and communications technologies including integrated circuit (IC) card, cryptograph, and telecommunication networks (Raja et al., 2008). Compare with traditional payment such as pay-by-check, pay-by-phone, or wire transfer, e-payment is considered more time- and cost-efficient, convenient, and flexible for customers and business (Sorkin 2001; Yu et al., 2002). New Internet payment methods based on wired and wireless Internet channels, along with related technologies such as smart cards, e-money, virtual currency (e.g., QQ coin, Facebook Credits) and P2P payment (e.g., Paypal), are together termed “e-payments.” Ways to make payments through the Internet or mobile phones...
have proliferated in the past few years. Various types of services exist, some of which are new methods of accessing existing payment arrangements, while others including both completely new payment arrangement and new methods of accessing existing payment arrangements, but all are ultimately linked to existing payment and banking channels (Allen, 2003).

Security is the main concern of online payment systems (Raja et al., 2008) which is working with Internet technology, they are in exposure of data theft, stealing, and fraud. Especially when the data about the money and financial information are more dangerous. If they lose a small piece of data such as personal identity, they may lose everything. Fraud risk refers to the global networks, credit, debit and charge cards can never avoid the risk of crime entirely (Levi & Burrows, 2008). E-payment fraud and computer crime found globally and reported fraud will increase. The e-payment method involves the disclosure of sensitive personal information online and the service providers may potentially misuses such personal information either purposely or accidentally (He & Mykytyn, 2007).

With the increasing usage of the Internet, the fears of privacy abuse become a top concern of most of the Internet users. The privacy issue becomes a conflicting issue between consumers and merchants. As consumers prefer to keep the details of their transaction private, conversely merchants and issuers in favor to ensure they capture and possess enough an appropriate and sufficient record of their transactions. E-payment may lead to an inadvertent error, intentional misappropriation of funds or fraudulently going out of business (Sorkin, 2001). Security refers to a set of procedures, mechanisms and computer programs to authenticate the source of information and guarantee the integrity and privacy of the information to abstain this circumstance to lead to a hardship of data or network resources. Online stores employ numerous safety cues to persuade customers to make an online purchase. During the online purchase process consumers come along and click through safety indicators such as privacy policies, product warranties, and customer reviewers (Noort et al., 2008). Web designers and B2C retailers extensively use logos, marks, seals, and signs of safety and security indicators. Will these safety cues result in favorable attitudes toward the site and toward the B2C retailers and increase individual confidence to make a payment electronically?

Although past researches (He & Mykytyn, 2007; Sumanjeet, 2009; Kim et al., 2010) were devoted to understanding individuals’ acceptance, more attention has been paid recently to individuals’ online behaviors at the post-consumption stages, which called post-consumption behaviors (Kim & Son, 2009). As with IS research, research on consumer behavior suggests that post-consumption behaviors are the key to a firm’s survival in the highly competitive marketplace (Kim & Son, 2009). Post-consumption behaviors of information systems are currently a more critical issue than ever before, especially in the context of B2C online services. This study thus extends the IS continuance model of Bhattacherjee (2001) with cue utilization theory (CUT), and thus this study attempts to adapt the original continuance use model with three constructs, perceived benefits, legal protection and risks to explore the effect of perception of web content and consumer’s post-consumption expectations on e-payment behavioral intention.

**E-PAYMENT LEGAL ACTS**

**Electronic Fund Transfer Act**

In the United States, the Electronic Fund Transfer Act (15 U.S.C. § 1693g (2004).) stipulates that if the identity of product users (consumers) can be verified by signature, photograph, or fingerprint, or by electronic or mechanical confirmation, the risk allocation of product users owing from being unable to verify(probably because of identity theft) cannot exceed the lesser of $50 or the unauthorized amount before the financial institutions reasonably realize the situation, except where the product users fail to report within sixty days (or in some extenuating