Available online at www.sciencedirect.com

ScienceDirect

Journal of Interactive Marketing 30 (2015) 1 – 19

JOURNAL OF INTERACTIVE MARKETING

www.elsevier.com/locate/intmar

Consumer Fear of Online Identity Theft: Scale Development and Validation

Patrick Hille [a,1] & Gianfranco Walsh [a,2] & Mark Cleveland [b,*,3]

[a] *Friedrich-Schiller University of Jena, Carl-Zeiss-Strasse 3, 07743 Jena, Germany*

[b] *The University of Western Ontario, DAN Management, Social Science Centre Room 4315, 1151 Richmond Street, London, Ontario N6A 5C2, Canada*

Available online 14 April 2015

Abstract

One unwelcome side effect accompanying the rise of e-commerce concerns the increase in cyber-crime, which in turn contributes to consumer fear of online identity theft (FOIT). This research details the development and validation of a FOIT scale that measures individual differences in consumers' proneness to feel negative emotions in relation to shopping online, specifically, the fear that others may illicitly use their identifying details. Based on literature insights, findings from qualitative interviews (n = 43), and three quantitative studies in Germany (n = 345, n = 539, n = 1,150) conducted in various online contexts, the authors propose a two-dimensional FOIT scale. Comprehensive validation procedures which involve relating FOIT to antecedents and consequences suggest the usefulness of the FOIT scale. Suggestions for future research and managerial implications are discussed.

© 2015 Direct Marketing Educational Foundation, Inc., dba Marketing EDGE. All rights reserved.

Keywords: Scale development; Fear of online identity theft; Cyber-crime; E-commerce; Misuse of personal and financial data; Purchase behavior

Introduction

> "Identity theft is the fastest growing form of consumer fraud in North America".
>
> [Cavoukian (2013, p 2).]

The myriad of routine transactions that are migrating to the Internet to the detriment of offline alternatives (e.g., travel, banking) in effect is forcing some consumers to transact online even against their preferences. The growth in online transactions coupled with the worldwide growth in Internet-based information exchange, social networking, the profusion of mobile devices, and e-commerce is accompanied by a concomitant rise in cyber-crime. This rise has made many consumers anxious about online identity theft (Acoca 2007; Reisig, Pratt, and Holtfreter 2009; Wall 2008) who consequently may refrain from conducting online transactions as a result of it. Online identity theft committed by cyber-criminals is the illicit use of another individual's identifying facts (name, birth date, credit card number, etc.) to perpetrate an economic fraud or masquerading identity on the Internet (Saunders and Zucker 1999). While identity theft also occurs offline (e.g., when identifying information is stolen from consumers' letterboxes), we focus on online identity theft because of the marked amplification of the amount of time and money spent in online environments. These increased online activities mean a further increase "in the amount [of] data trails people leave online" (Priem et al. 2011, p 47) that identity thieves try to access and exploit.

As exemplified by the recent data breach involving millions of customers of *Target* (a major US retailer) (Harris et al.

* Corresponding author.

E-mail addresses: patrick.hille@uni-jena.de (P. Hille), walsh@uni-jena.de (G. Walsh), mclevela@uwo.ca (M. Cleveland).

[1] Patrick Hille is a *PhD Candidate*, General Management & Marketing, Faculty of Economics and Business Administration, Friedrich-Schiller University of Jena (Germany).

[2] Gianfranco Walsh, PhD, is *Professor of General Management & Marketing*, Faculty of Economics and Business Administration, Friedrich-Schiller University of Jena (Germany).

[3] Mark Cleveland, PhD, is *Dancap Private Equity Professor of Consumer Behavior*, DAN Management and Organizational Studies, University of Western Ontario (Canada).

http://dx.doi.org/10.1016/j.intmar.2014.10.001

1094-9968/© 2015 Direct Marketing Educational Foundation, Inc., dba Marketing EDGE. All rights reserved.

2014), identity theft is one of the fastest growing crimes of the 21st century. In highly industrialized countries, it is also ranked as one of the main reasons for consumer complaints (Unisys 2011; van der Meulen 2006). In the U.S., identity theft ranked first in 2009, with 21% of the more than 1.3 m complaints reported by consumers to the *Federal Complaints Commission* being related to identity theft (FTC 2010). Also, in the U.S. alone, there were more than 12 m victims of identity theft in 2012 (4% of the population) with a total incurred damage of $21bn (Rogers 2013). Alongside financial risk, consumers fear the reputational damage (e.g., being publicly associated with illicit products) arising from online identity theft (Eisenstein 2008; Lynch 2005), pointing to a two-dimensional conceptualization of the construct.

Given the endemic nature of online identity theft it is not surprising that nearly 70% of U.S. Internet users believe that they are at a higher risk of becoming a victim of a cyber-crime than of a physical crime (Reisig, Pratt, and Holtfreter 2009). This fear, fed by the realization that their personal data is valuable to identity thieves (Coles-Kemp, Lai, and Ford 2010; Kieschnick, Aukerman, and Shorter 2006), leads to adjustments in consumers' Internet behaviors, including disinclination to share personal information online, as well as reduced intentions to purchase online (e.g., Grau 2006; Leyden 2005).

From both practical and research standpoints, what cannot be measured cannot be managed. Although the notion of fear is frequently discussed in relation to consumer online shopping (e.g., LaRose and Rifon 2007; Miyazaki and Fernandez 2001; Rust, Kannan, and Peng 2002), scholars thus far made no attempt to measure it. Despite increasing anecdotal and empirical evidence regarding the existence of consumers' fear of online identity theft (hereafter, FOIT), the extant literature is inadequate. Knowledge about FOIT-associated behavior derives from heterogeneous, often anecdotal sources. The extant studies on the topic are either qualitative (e.g., Poddar, Mosteller, and Ellen 2009) or use overly parsimonious measures that inadequately reflect the conceptual breadth of FOIT (e.g., European Commission 2012), which limits the generalization of the findings. For example, Roberts, Indermaur, and Spiranovic's (2013) study on the predictors of fear of cyber-identity theft employs only two items to measure the concept, even though these authors assert that identifying and managing FOIT requires a reliable measurement scale. However, thus far, no such scale exists. The absence of such a scale impedes the task of comprehensively assessing consumers' FOIT as a potential basis for market segmentation; as well as for developing strategies to address and serve particular groups, based on the degree to which consumers' aversion of identity theft is salient and/or predictive of behavior. Furthermore, as a consequence of the lack of an accepted scale, empirical research regarding FOIT outcomes remains underdeveloped. Indeed, evidence of consumer FOIT mainly consists of testimonials from affected consumers, or the pronouncements of IT risk experts and non-governmental organizations (e.g., Gooch 2007; Kempf 2009; Unisys 2011).

The primary purpose of this research is to develop and validate a scale for measuring FOIT, which we theoretically define as *an emerging negative consumer emotion activated through consumers' cognitive appraisal/own thoughts regarding the possibility of the theft of personal and financial data when conducting transactions online, which can also be generated by external stimuli (*e.g.*, media reports thereof), which can then influence consumers' online behavioral outcomes*. The present research encompasses qualitative research, in order to bolster the emerging literature-based notion that FOIT is a two-dimensional construct. The applicability of the construct is enhanced by embedding the construct theoretically within a network of antecedents and consequences thereby establishing the FOIT scale's predictive and nomological validity. To this end, three quantitative studies are employed to develop, validate and test our scale within a nomological net of related constructs, including purchase intention. The FOIT scale should be applicable across different e-commerce contexts and possibly even to the domain of non-online shopping. We conclude with a discussion of theoretical and managerial implications as well as highlight directions for future research.

Theoretical Background

When using the Internet for commercial purposes, consumers have to transfer their personal and financial data to merchants or third parties in order to carry out online business transactions (Forsythe et al. 2006). Personal and financial data combined constitute a person's unique online identity. The expanding scope and frequency of online engagement and an increasing number of consumer-specific data points thus amplify the possibility that this information could be misused (Mitchison et al. 2004). Not surprising, the literature has alluded to consumer online fear for some time. For example, Wang, Lee, and Wang (1998) argue that Internet customers perceive fear and distrust regarding the loss of personal privacy in online transactions. In their frequently-cited article, Miyazaki and Fernandez (2001, p 41) refer to consumers' "security fears" and Rust, Kannan, and Peng (2002) refer to "privacy fears." Westin (2003, p 445) alludes to "fears about the security of using credit cards to shop online" and Xu and Gupta (2009, p 141) mention the "fear of losing control over personal information." Therefore, numerous scholars in the field acknowledge the existence of "fear", even though they make no attempt to measure it.

Long recognized as a serious threat to privacy and financial security, consumers' heightened sense of vulnerability due to identity theft can lead to changes in consumers' online behaviors (Gartner 2005; Milne, Labreque, and Cromer 2009). Prior research alludes to consumer FOIT, yet only few studies specifically investigate resulting behavioral outcomes (e.g., Brant 2009; Sproule and Archer 2010). Recently, Roberts, Indermaur, and Spiranovic's (2013) exploratory research identified five significant predictors of "fear of cyber-identity theft" such as age, fear of more conventional place-based crime, Internet views crime (i.e., the importance of the Internet for informing views of crime trends and the criminal justice system), Internet use at home, and Internet use frequency. However, drawing substantive conclusions from the study is limited, because the authors did not develop a scale that comprehensively captures the distinct facets of consumers' FOIT, although a compelling case can be

Download English Version:

https://daneshyari.com/en/article/885975

Download Persian Version:

https://daneshyari.com/article/885975

Daneshyari.com