INTRODUCTION

Internet technology facilitates “faceless” transactions. At the same time, a new set of risks arises. In this article, we focus on the Internet-related risks associated with identity theft. Specifically, our objectives are to explain electronic-based identity theft (i.e., cyber-identity theft) and to explore the impact of cyber-identity theft on consumers, businesses, organizations and public policies. Our article makes two specific contributions to the identity theft literature: (a) it explains identity theft as it relates to the Internet and (b) it defines key methods of cyber-identity theft.

BACKGROUND

We first present a brief background on this emerging issue. Identity theft is broadly defined as the practice of using the identity of another to obtain credit (Sovern, 2004). Specific to U.S. federal law, identity theft is the “unauthorized use of another person’s identification with the intent to commit another crime” (U.S. Code, Chapter 47, Title 18). Any individual who violates federal identify law and obtains money or property valued at or over $1,000 over a one year period may be sentenced to up to 15 years in prison.

In extant studies, attention primarily focuses on legal aspects and avenues for future legislation and policy. Linnhoff and Langenderfer (2004) review the Fair and Accurate Credit Transactions Act (FACTA). As the 2003 Act currently stands, most of the financial risk is borne by the victim (Sovern, 2004). Simply stated, identity theft victims bear most of the costs of reestablishing their “good names” after an identity theft. Notably, some purchases made by identity thieves show up on the victim’s credit report and may be difficult to remove. Critics claim that, at present, the law provides insufficient incentives for financial institutions to take preventative measures against identity theft (Lee, 2001; Sovern, 2004). Sovern (2004) argues that consumers should stand up to credit bureaus and creditors who fail to delete fraudulent transactions from victims’ credit reports.

Identity theft has the potential to wreak havoc on consumers’ social and financial lives. At present, U.S. consumers have rather extensive access to public records (e.g., birth certificates, marriage certificates, tax documents), and consumers may be reluctant to sacrifice these rights. For instance, a survey conducted at Washington State University finds that a majority of individuals in the state of Washington support continued individual access to public records (Cuillier, Passey, & Hinz, 2003), despite the presence of identity theft. Similarly, business organizations do not welcome laws concerning their security policies (Knowledge at Wharton, 2005; Lacey & Cuganesan, 2004).

Next, we explore how identity theft relates to the Internet. Cyber-identity theft involves the use of electronic (e.g., via the Internet) means to carry out any form of identity theft. Close et al. (2004, p. 48) define cyber-identity theft as “the online or electronic acquisition of personal information with the purpose of utilizing such information for deceitful activity either on the Internet or offline.”

Currently, cyber-identity theft is the most common Internet-related crime reported to the U.S. Federal Trade Commission (FTC). Victims of cyber-identity theft often suffer socially, psychologically and financially. Businesses and organizations are also victimized by this type of Internet crime.

Academic research is beginning to emerge on the topic of identity theft; however, to date scholars have published relatively few studies specific to Internet-related identity theft. Close et al. (2004) present an overview of cyber-identity theft with an emphasis on the implications for public policy. Policy and online behavior must change to combat cyber-identity theft. Internet-related identity theft is, in part, a function of an individual’s risky