Chapter 77
Internet Fraud

Michael Bachmann
Texas Christian University, USA

Brittany Smith
Texas Christian University, USA

ABSTRACT

This article provides an introduction into the topic of Internet fraud. A precise definition and detailed descriptions of the most prevalent Internet fraud schemes are provided. The entry presents a history of frauds committed on the Internet and introduces the leading scholars on the subject. Predominant areas of research are discussed, and future directions of the problem of Internet fraud schemes are outlined. The entry concludes with a critique of current limitations and advancements needed to better address the increasing problem of online frauds.

INTRODUCTION

In legal terms, "fraud" is typically defined as a false representation by means of any act, expression, omission, or concealment made knowingly or recklessly to deceive another to one's advantage. The terms "Internet fraud" or "e-fraud" generally denominate any usage of interconnected computerized or computer-assisted electronic networks or services for any type of fraudulent scheme that intentionally deceives prospective victims through false representation, thereby intending to solicit, obtain, or transmit fraudulent transactions that deprive victims of personal property or any interest, estate, or right. Simply stated, Internet fraud can be understood as any usage of computerized networks, oftentimes in conjunction with social engineering tactics intended to deceive or manipulate a victim in order to give the offender a material advantage at the victim's expense. Unlike victims of violent crime, fraud victims are not forced to give up their possessions; rather, they are deceived, coerced, or otherwise manipulated into giving them up voluntarily (Gottfredson & Hirschi, 1990).

Internet frauds largely mirror previous fraud schemes perpetrated over the phone or through the mail (Computer Crime Research Center, 2005).

DOI: 10.4018/978-1-4666-0315-8.ch077

While some researchers (e.g. Wall, 2001) argue that from a strictly legal standpoint, Internet fraud schemes are essentially the same as 'old-fashioned' frauds committed with new tools and nothing more than the "same old wine in new bottles" (Grabosky, 2001, p. 243), there is broad consensus among criminologists who examine the social-structural conditions of electronic environments that society is confronted with a qualitatively new generation of fraudulent schemes. The improved quality of online scams arises primarily from three general features of social interactions taking place within the world of connected computers that render them markedly different from the ones taking place in the 'meatspace' (Pease, 2001, p. 23).

Most notably, the Internet "variously 'transcends', 'explodes', 'compresses', or 'collapses' the constraints of space and time that limit interactions in the 'real world'" (Yar, 2006, p. 11). It represents the most important element for the "time-space compression" of globalization in that it allows instantaneous interactions between spatially distant actors (Harvey, 1989). This feature of cyberspace has important implications for fraud schemes because it grants "e-fraudsters" unprecedented access to potential victims from all around the globe.

Secondly, the Internet offers varying degrees of automatization in interaction (Shields, 1996). Among other aspects, automated interactions within computer-mediated communication networks extend both the scope and scale of fraudulent schemes. Many-to-many communications inexorably alter the relationship between fraudsters and their victims and they hinder the efforts of criminal justice systems to investigate, counteract, or resolve the scams (Capeller, 2001). On the one side, Internet users are instantaneously targetable by a substantially large pool of potential fraudsters from all over the world. Concurrently, the offenders are no longer bound by the limits of physical proximity and can launch their schemes through highly automated routines. They possess a multitude of software tools in their cache that permit them to distribute deceptive or misleading information, to create increasingly sophisticated websites that contain fraudulent material or fake logins, and to remain undetectable to law enforcement.

A third criminogenically relevant feature of computer networks is that they allow for easy creation, alteration, and reinvention of the social identity. Internet users can create arbitrary virtual avatars, electronic personas that are often markedly different from their 'real world' identities (Turkle, 1995). The ability to disguise social identity in the electronic realm is of high criminological relevance because it allows potential fraudsters to remain largely anonymous (Snyder, 2001). The increased anonymity in computerized networks reduces the offender's perception of the risks involved in the commission of Internet frauds, which ultimately increases the likelihood that the fraud is committed (Joseph, 2003).

Combined, these three aspects of social interactions in online environments exponentially multiply the possibilities for potential offenders to target vast numbers of potential victims and their property to a previously unknown degree. They render the Internet the ideal "breeding ground for fraud" (Fried, 2001, p. 1). While the crime of fraud is not new and has been around for centuries, the invention and proliferation of the Internet has opened a Pandora's Box for a new breed of criminal to take advantage of unsuspecting or unaware victims.

OVERVIEW

Intellectual History of Internet Fraud

Prior to the commercialization of the Internet in the early 1990s, only a few computer-mediated or computer-oriented fraud cases, usually committed through impersonation or other social engineering methods, had been recorded. A notorious case originated in 1970 when Jerry Neal Schneider began gathering documents from the Pacific