Routledge
Taylor & Francis Group

Victims & Offenders

An International Journal of Evidence-based Research, Policy, and Practice

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uvao20

The Changing Face of Financial Crime: New Technologies, New Offenders, New Victims, and New Strategies for Prevention and Control

Donald Rebovich

To cite this article: Donald Rebovich (2021) The Changing Face of Financial Crime: New Technologies, New Offenders, New Victims, and New Strategies for Prevention and Control, Victims & Offenders, 16:3, 283-285, DOI: 10.1080/15564886.2021.1876196

To link to this article: https://doi.org/10.1080/15564886.2021.1876196

Published online: 16 Feb 2021.

VICTIMS & OFFENDERS
2021, VOL. 16, NO. 3, 283–285
https://doi.org/10.1080/15564886.2021.1876196

Routledge
Taylor & Francis Group

The Changing Face of Financial Crime: New Technologies, New Offenders, New Victims, and New Strategies for Prevention and Control

Donald Rebovich

Professor, School of Business and Justice, and Executive Director, The Center for Identity Management and Information Protection (CIMIP), Utica College, Utica, New York, USA

Financial crime is a growing crime problem throughout the world. It is a trillion-dollar industry that takes an enormous social and economic toll on the lives it touches. The primary goal of this special issue was to explore the many dimensions of financial crime from the perspectives of victims (both individual and organizational) and offenders. We were particularly interested in aspects of financial crime that are focused on the evolution of methods of financial crime facilitated through technological advances, vulnerable groups being exploited by offenders, and the consequences of financial crime victimization. Finally, we were interested in prevention and enforcement strategies utilizing new technology to address the problem of financial crime. For each of these topic areas, international submissions were encouraged. We received submissions from around the globe from academia, as well as from private and public sector entities.

The focus of our special issue is on the impact of new technology on financial crime. The articles included in this issue examine a wide range of topics related to financial crime commission, victimization, prevention, and control. Authors address timely issues and questions such as: How has technology hastened the growth of financial crime both nationally and internationally? In what environments are financial crime most likely to flourish? What part does organized crime play in financial crime activities? What are the groups most susceptible to being victimized by enterprising perpetrators of financial crimes, and why? And, what role can society play in enhancing efforts to prevent financial crime victimization in the future?

Organization of the special issue

One of the primary themes of the special issue is how advances in technology have become a central force in bolstering the abilities of fraudsters to exploit the weaknesses of potential victims, enabling offenders to capitalize on a lack of preventive knowledge by certain groups, thus opening these groups to criminal exploitation.

The lead article focuses on the effects of such exploitation on the business community. In this article, David Buil-Gil, Nicholas Lord and Emma Barrett analyze the dynamics of online business activities, cybersecurity measures and cyber-victimization. Their article spotlights how digital space and digital systems are a core operating context for most businesses and

CONTACT Donald Rebovich drebovich@utica.edu The Center for Identity Management and Information Protection (CIMIP), 105 ECJS Building, School of Business and Justice, Utica College, Utica 13502, New York.

associated activities, whether entering into economic relations with customers purchasing goods and services, storing and sharing information, or undertaking commercially sensitive activities that involve confidential data. Consequently, as pointed out by the authors, cybersecurity becomes a primary concern for businesses operating within digital (and often) global economies. The authors of this piece explain how digital space offers new opportunities for varied financial crimes, including frauds, that may be enabled by, or dependent on, internet-connected systems. The most common crime types identified include business e-mail compromise and e-mail account compromise, nonpayment and non-delivery fraud, and investment scams.

In the next article, Adam Ghazi-Tehrani and Henry Pontell zero in on electronic "phishing", the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity via electronic communication. The authors describe how this form of victim exploitation has quickly evolved beyond original low-skill schemes that relied on casting "a wide net." They find that the frequency of all types of phishing has risen dramatically in recent years. Their study expounds upon the current state of phishing, the expected technological advances and developments in the near future, and the best prevention and enforcement strategies that can effectively be implemented. Their research is based on interviews with approximately 60 information technology security professionals, "hackers," and academic researchers.

The next technology-oriented article, by Claire S. Lee spotlights victimization in one of the most densely populated nations in the world with a rapidly growing financial crime problem: China. When it comes to online populations and markets, China has some of the largest in the world. As a result, Chinese cybercriminals have more opportunities to target and access victims. While recent research in Western countries has examined internet fraud victimization and offenses in virtual communities, a relatively small body of research on these phenomena has been conducted in non-Western societies. Lee's research attempts to address this research shortfall by analyzing internet fraud victimization in Chinese online communities

The fourth article selected for our special issue examines how bitcoin and ransomware can serve as new financing sources for terrorists. Authors Hannarae Lee and Kyung-shick Choi note early on that conveniences afforded to all from technological development have been reached at an astonishing level with the invention of cryptocurrencies like bitcoin being at the forefront. They argue that the same unique characteristics of bitcoin that attract the general public may also attract criminals (e.g. cybercriminals and terrorists) looking for a fast and convenient way of transferring money. Since cybercriminals usually demand their ransom using bitcoin, the unlawful use of bitcoin can be tied to the increase in ransomware attacks in recent years. Due to this apparent connection, there is continued speculation about the relationship between terrorist activities and the use of bitcoin. Their article analyzes the dynamic properties of bitcoin prices, ransomware attacks, and terrorist activities, using three different data sources. To measure the changes in bitcoin price, the authors analyzed daily bitcoin trading data from the Yahoo Financial website for a seven year period along with search queries from Google and Wikipedia, and trend data from the Global Terrorism Database (GTD).

New victims of financial crime are the focus in our next two articles. Those in the military are examined as ripe targets for fraud via the use of dating sites as a lure for the commission of "romance fraud." Casandra Cross and Thomas Holt note that in 2019, romance fraud was

one of the highest categories of financial loss associated with fraud in many countries. The authors examine romance fraud reports made by individuals to Scamwatch (an Australian fraud reporting portal). During a thirteen-month review period, in I in 8 reports, offenders were identified as having employed the military narrative to target victims. This article examines the ways that the military narrative is used by romance fraud offenders and analyzes both those who were initially targeted and those who were successfully defrauded.

The elderly were the targeted financial crime victimization group examined in the next article included in our special issue. Criminal cases from the U.S. Postal Inspection Service (USPIS) were analyzed by authors Donald Rebovich and Leslie Corbo and researchers from the Identity Management and Information Protection Center (CIMIP) of Utica College. The study centered on frauds committed against victims aged 55 years and older with the primary objective being to uncover key empirical information on characteristics of victims of elderly fraud, those who commit these crimes, and the methods they employ to commit these fraudulent acts in order to develop characteristic profiles for each category to serve as the foundation for fraud awareness programs. One of the key findings they report is that elderly fraud cases in which the technological naivete of victims was manipulated by group offenders using multiple methods of attack were the most successful in defrauding senior citizens.

The final two articles in our special issue describe new strategies and initiatives designed to either prevent or control this new generation of financial crimes. First, Jay Albanese examines the role of organized groups in the commission of financial crimes, focusing on financial crime cases actually investigated and prosecuted that involved organized crime groups. Dr. Albanese contends that what has been sorely lacking thus far is a comparison of actual cases of organized crime (i.e., investigated and prosecuted) to determine the extent to which organized crime prosecutions parallel the nature of larger policy debate and typologies about the various types of organized crime that pose the greatest public threat. Data are presented to examine the extent to which the policy and research discussions about organized crime match the organized crimes found in practice. In the article, the author stresses that what has been lacking thus far is a examination of actual cases of organized crime (i.e., investigated and prosecuted) to determine the extent to which organized crime prosecutions parallel the nature of larger policy debate and typologies about the various types of organized crime that pose the greatest public threat. The article attempts to answer the question – Does the nature of organized crime reflected in the research literature match the nature of organized crime investigated and prosecuted by authorities?

For the last special issue article, identity crime serves as the centerpiece for a dissection of how professionals from the field can be at the forefront of exploring effective efforts for preventing identity theft and identity fraud. Authors Nicole Piquero, Alex Piquero, Stephen Gies, Brandn Green, Amanda Bobnis and Eva Valasquez emphasize that identity crime is one the fastest growing economic crimes in the U.S. with an estimated 26 million American citizens per year falling victim to various forms of identity-based crimes. The authors' study contributes to the scholarship on financial crimes facilitated through identity-based criminal activity. The authors examine the views on technological approaches to the prevention of identity theft among 50 professionals working in identity-based crime victim services, including those from the public sector and private industry. Interviews of these industry "insiders" are the source of valuable insights into the most effective paths to take in the quest to prevent future identity crimes.