White-Collar Crime Online

Deviance, Organizational Behaviour and Risk

Petter Gottschalk · Christopher Hamerton

palgrave
macmillan

White-Collar Crime Online

Petter Gottschalk · Christopher Hamerton

White-Collar Crime Online

Deviance, Organizational Behaviour and Risk

palgrave
macmillan

Petter Gottschalk
Department of Leadership
and Organizational Behaviour
BI Norwegian Business School
Oslo, Norway

Christopher Hamerton
Sociology, Social Policy and Criminology
University of Southampton
Southampton, UK

ISBN 978-3-030-82131-9 ISBN 978-3-030-82132-6 (eBook)
https://doi.org/10.1007/978-3-030-82132-6

Cover credit: Ronnie Li/Getty

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

List of Figures

1

Introduction

White-collar offenders are privileged individuals who abuse their legitimate access to resources to commit and conceal their financial crime (Benson, 2020; Dodge, 2009; Friedrichs et al., 2018; Piquero and Schoepfer, 2010; Pontell et al., 2014; Stadler et al., 2013; Sutherland, 1939, 1983). Traditionally, white-collar offenders have worked offline when committing and concealing corruption, fraud, theft, manipulation, and other forms of financial crime. As documented in this book, working online is not only a matter of opportunity; it is also a matter of motive and willingness. For example, the distance created by working online, and the possibility of anonymity and fake identity might influence the willingness for deviant behavior. White-collar offenders online commit cybercrime through legitimate professions in privileged positions.

This book addresses cybercrime committed through legitimate professions. The book applies the offender-based perspective on white-collar crime. The offender-based perspective emphasizes characteristics of actors such as social and professional status, respectability, and power (Dodge, 2009; Friedrichs et al., 2018; Piquero & Schoepfer, 2010; Pontell et al., 2014, 2021; Stadler et al., 2013; Sutherland, 1939, 1983). The offender-based definition emphasizes some combination of the

P. Gottschalk and C. Hamerton, *White-Collar Crime Online*,
https://doi.org/10.1007/978-3-030-82132-6_1

actors' high social status, power, and respectability as the key features of white-collar crime (Benson, 2020). As evidenced by Payne and Hadzhidimova's (2020) review of cybercrime research, the offender-based perspective has been completely absent from the research agenda.

The integrated and deductive theory of convenience applies offender-based rather than offense-based perspectives on acts of white-collar crime by implicating individual and organizational motive for illegitimate financial gain, opportunities for crime in organizational settings, and personal willingness to engage in deviant behavior (Braaten & Vaughn, 2019; Chan & Gibbs, 2020; Hansen, 2020; Kireenko et al., 2019; Vasiu & Podgor, 2019). The convenience triangle thus consists of financial motive, organizational opportunity, and personal willingness (Gottschalk, 2020).

This book addresses a gap in the literature in the area of white-collar computer crime termed white-collar offenders online in the perspective of convenience theory. The book explores technology-aided white-collar crime caused by professional deviance. White-collar crime committed using technology has its special convenience characteristics. The book advanced the novel theoretical approach of convenience theory that was introduced only a few years ago (Gottschalk, 2020; Vasiu & Podgor, 2019). The book explores the intersections of white-collar crime and cybercrime. The book combines insights from organizational behavior, information technology, management, business administration, psychology, sociology, and criminology. The book explores white-collar crime from the perspective of online crime and discusses the various motives, opportunities, and behaviors. Convenient white-collar crime online is a unique concept that advances insights into the convenience of cybercrime for members of the elite in society. The digitally embedded workplace has its unique characteristics that influence the extent of crime convenience (Teubner & Stockhinger, 2020: 1):

> Although driven by technology, digitalization is not a mere technological phenomenon but has fundamental economic and societal consequences that can be seen in many aspects of our professional and private lives.

This book brings together two significant domains of criminological inquiry and research, namely those dealing with white-collar crime and with cybercrime. The two combined domains are studied in the perspective of convenience theory.

This book applies the term cybercrime as computer-oriented crime, which is crime that involves a computer and a network (Kshetri, 2005). The computer may be used as an instrument in the commission of crime, and it may be the target of crime. Cybercrime is not limited to the cyberspace, which is describing a widespread, interconnected digital technology. Rather, insider attacks on technologies of database management and information storage are just as much cybercrime as are attacks on the internet and the World Wide Web, as well as Facebook and other online services. In response, a new discipline named cyber criminology emerged with Jaishankar (2007) defining cyber criminology as the study of causation of crime that occurs in the digital space and its impact on the physical space.

Like so many other terms in research, there is still no precise and clear definition of cybercrime in academic contexts. Some call it electronic crime, computer crime, computer-related crime, hi-tech crime, technology-enabled crime, e-crime, or cyberspace crime (Sarre et al., 2018). With our focus on white-collar offenders online, it is not an issue to attempt to distinguish the various terms from each other. White-collar offenders commit both cyber-dependent crime and cyber-enabled crime. A cyber-dependent crime, sometimes labeled true cybercrime, is an offense that cannot occur without computer and network technology (Akdemir & Lawless, 2020). The case study of movie piracy in this book is an example of cyber-dependent crime (Borgarting, 2019; Høyesterett, 2019; Stone, 2015) similar to music piracy (Hinduja, 2012; Popham & Volpe, 2018).

When studying cyber fraud, Drew and Farrell (2018) distinguished between cybercrime that is directed at computers and related technology and cybercrime where technology is an enabler and integral part of the offense. Cyber fraud offenses under the first category include illegal access, illegal interception, data interference, system interference, misuse of devices, and hacking offenses. Cyber fraud offenses under the

second category include advance fee fraud, investment scams, fraudulent financial transactions, and identity theft.

White-collar offenders online commit both occupational crime and corporate crime. The professional dimension of white-collar crime becomes particularly evident when financial crime is committed to benefit the organization rather than the individual. This is called corporate crime as opposed to occupational crime for personal benefit (Bittle & Hébert, 2020). Hansen (2009) argues that the problem with occupational crime is that it is committed within the confines of positions of trust and in organizations, which prohibit surveillance and accountability. Heath (2008) found that individuals who are further up the chain of command in the firm tend to commit bigger and more severe occupational crime. Corporate crime sometimes labeled organizational offending, on the other hand, is resulting from offenses by collectivities or aggregates of discrete individuals. If a corporate official violates the law in acting for the corporation, we still define it as corporate crime. However, if he or she gains personal benefit in the commission of a crime against the corporation, we regard it as occupational crime. A corporation cannot be subject to imprisonment, and therefore, the majority of penalties to control individual violators are not available for corporations and corporate crime. Detected corporate crime can harm executives involved, since "corporate outcomes such as misconduct serve as signals of the underlying quality of the individuals employed by the firm" (Naumovska et al., 2020: 883).

An example of corporate crime is online consumer fraud. White-collar offenders as legitimate online marketplace participants facilitate fraudulent transactions using various tactics (Harrison et al., 2020: 61):

> These include deception tactics where deceivers create inaccurate representations, negotiation tactics that are used to coerce victims into purchasing nonexistent or overpriced gods, and shill bidding by a fraud perpetrator or his conferates to inflate the selling price of goods.

By limiting attention to computer crime as financial crime by white-collar offenders, we focus on the profit-orientation of such crime. This definition excludes incidents of computer crime to cause damage without

a gain, and it excludes incidents of computer-assisted financial crime by people who do not have legitimate access to premises, resources, and systems in professional settings. For example, Nigeria-related financial crime is extensive and 122 out of 138 countries at an Interpol meeting complained about Nigerian involvement in financial fraud in their countries. The most notorious type of non-white-collar crime attempted daily on office workers all over the world is probably the so-called advance fee fraud (Dion, 2010; Webster & Drew, 2017). The sender will seek to involve the recipient in a scheme to earn millions of dollars if the recipient pays an advance fee (Ampratwum, 2009). Even if malware infection, hacking, and other incidents are frequently reported in the popular press (Hagen et al., 2008), these kinds of computer crime are only of interest here if they have a profit motive. Computer crime is here profit-driven crime to gain access to and control over assets that belong to someone else.

While cybercrime is a criminological domain of computer-oriented and -enabled offences, white-collar crime is a criminological domain of occupationally and organizationally based offences. These two areas are the subject of concerted consideration in tandem in this book and studied in the perspective of convenience theory.

White-collar offenders online are trusted cybercriminals, who abuse trust to commit and conceal financial crime. Trust is a general characteristic of all white-collar offenders (Hamerton, 2020; Hansen, 2009; Jordanoska & Schoultz, 2020; Kempa, 2010; Podgor, 2007). Trust is an important contribution to the convenience of white-collar crime. Dearden (2016) argues that violation of trust is at the core of white-collar crime opportunity. Trust implies that vulnerability is accepted based upon positive expectations of the motives and actions of another. Controlling a trusted person is often considered both unnecessary and a signal of mistrust. In many cultures, the opposite of showing trust is to monitor and question what a person is doing. For example, a board can tell management what to do, but they do not tell them how to do it. The board shows trust that management will do it in an acceptable manner. If the board would move from only controlling what management has done to how management did it, then it might be perceived as mistrust. Yip et al. (2013) argue that trust is a mechanism for people to cope with

risk and uncertainty in interactions with others. Kim et al. (2009: 401) define trust as "a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behavior of another". The positive expectations can relate to what another does, how it is done, and when it is done. The positive expectations can relate to the reaction of another, where it is expected that the reaction will be understandable, acceptable, and favorable. Vulnerability means that trust can easily be violated without detection or correction of deviant behavior. Trust is associated with dependence and risk (Chan et al., 2020: 3):

> The trustor depends on something or someone (the trustee or object of trust), and there is a possibility that expectations or hopes will not be satisfied, and that things will go wrong. Trust is not absolute, but conditional and contextual.

Just like the concept of trust is relational, such that trust inherently requires a target, so too is the concept of felt trust relational. It is the felt trust that can influence an individual's tendency to crime, while it is the actual trust that is part of the opportunity structure for crime. The gap between the two represents how accurately people understand others' perceptions of them (Campagna et al., 2020: 994):

> The concept of felt trust reflects what the more general interpersonal perception literature refers to as a dyadic meta-perception – one person's belief about the thought, attitude, or perception held by another person.

Uygur (2020) studied fraud in the charity sector in England and Wales. He analyzed 42 fraud and 42 no-fraud charities. His findings suggest that excessive trust towards the charities creates the opportunity for fraud to take place. Similarly, Gottschalk (2017: 121) studied detection and neutralization of economic crime in religious organizations and phrased the following question:

> Are there too much trust, too much freedom, too much individual authority, too little skepticism, too much loyalty, and too little control of the financial side in religious organizations?

Gottschalk and Gunnesdal (2018) have estimated a detection rate for white-collar crime of less than one out of twelve offenders in Norway, which seems supported by an empirical study of bribery detection in Norway by Andresen and Button (2019). The detection rate in the United States seems even lower based on estimates of the magnitude of white-collar crime by the National White-Collar Crime Center (Huff et al., 2010) and the Association of Certified Fraud Examiners (ACFE, 2008, 2014, 2016), which estimates the total annual loss from white-collar crime to be between $300 and $660 billion (Wall-Parker, 2020). Offenders tend to move under the radar (Williams et al., 2019). This book documents that the detection rate for white-collar offenders online certainly must be even lower than the detection rate for white-collar offenders who operate offline.

As argued by Walburg (2020: 343), too little insight exists about the extent, structures, and development of white-collar crime and its multifaceted varieties, especially when it comes to corporate crime:

> (…) this is largely explicable by the well-known and persistent difficulties of measuring undetected acts of corporate wrongdoing (…)

Even when an observer believes to have noticed a crime signal, the observer can be reluctant to report the observation (Bjørkelo et al., 2011; Bookman, 2008; Bowman & Gilligan, 2008; Bussmann et al., 2018; Mpho, 2017). In most countries, there are no benefits from reporting misconduct and crime in the organization (Brown et al., 2016; Keil et al., 2010). Rather, retaliation and reprisals can be the result for the observer (Mesmer-Magnus & Viswesvaran, 2005; Park et al., 2020; Rehg et al., 2009; Shawver & Clements, 2019). This book documents that the whistleblowing rate for online incidents certainly must be even lower than the whistleblowing rate for offline incidents.

Therefore, white-collar crime can remain conveniently concealed even when others have noticed and observed it (Bussmann et al., 2018). Lack of trust in the legitimacy, capacity, and competence of the police and the criminal justice system in general causes a further reduction in the willingness to blow the whistle on observed wrongdoing (Tankebe, 2019).

This book has the following structure. Chapter 2 introduces the theory of convenience that is applied throughout the book. The theory suggests that crime convenience can be found in three dimensions: the financial motive where the offender conveniently can benefit from possibilities and avoid threats, the professional convenient opportunity to commit and conceal crime, and the personal willingness for convenient deviant behavior.

Chapter 3 focuses on characteristics of online convenience for white-collar offenders. A distinction is made between outsider business cybercrime and insider business cybercrime. Some cases from the Cambridge cybercrime database are presented.

Chapter 4 presents a number of case studies of outsider business cybercrime. The cases cover movie piracy, foreign aid fraud, crypto currency crime, industrial espionage, Covid-19 fraud, and CEO fraud.

Chapter 5 presents a number of case studies of insider business cybercrime. The cases cover embezzlement, money laundering, internal bank fraud, and accounting manipulation. In addition, gendered white-collar crime is discussed.

Chapter 6 raises a number of technology issues related to white-collar offenders online. The first issue is the digitally enabled identity gap, where an offender randomly or intentionally has a different identity online compared to the real-world identity. The second issue is special characteristics of the internet that set online offenses apart from offline offenses. The third issue is online crime terminology, where not only offender language can help disguise wrongdoing, but also underground terminology can prevent people from understanding what is going on. The fourth technology issue is special services in terms of infrastructure and software that is available on underground markets to help commit and conceal white-collar online crime. White-collar offenders can engage in crime online without high-level technical skills.

Chapter 7 discusses policing cybercrime including law enforcement approaches, digital forensics, and intelligence strategy, as well as detectives as knowledge workers. Chapter 8 continues on the path of knowledge workers by introducing theoretical knowledge requirements as well as empirical knowledge requirements to detect, investigate, and prosecute cybercriminals.

Chapter 9 introduces a completely different, yet well-researched group of cybercriminals for comparison. The chapter is concerned with online child grooming where pedophiles attract children for sexual abuse. While some of the aspects of child grooming are very different from white-collar crime, there are interesting issues related to stages in the criminal process as well as the existence of social communities of offenders online where analogy is relevant for discussion.

Chapter 10 introduces three offline case studies for comparison. The case studies are from Austria, Congo, and Denmark describing recent internal investigations into suspicions of white-collar crime.

References

ACFE. (2008). *2008 Report to the nations on occupational fraud and abuse*. Association of Certified Fraud Examiners.

ACFE. (2014). *2014 Report to the nations on occupational fraud and abuse, 2014 Global Fraud Study*. Association of Certified Fraud Examiners.

ACFE. (2016). *CFE code of professional standard*. Association of Certified Fraud Examiners. www.acfe.com/standards/

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimization: A lifestyle routine activities approach. *Internet Research, 30*(6), 1665–1687.

Ampratwum, E. F. (2009). Advance fee fraud "419" and investor confidence in the economies of sub-Saharan African (SSA). *Journal of Financial Crime, 16*(1), 67–79.

Andresen, M. S., & Button, M. (2019). The profile and detection of bribery in Norway and England & Wales: A comparative study. *European Journal of Criminology, 16*(1), 18–40.

Benson, M. L. (2020). Theoretical and empirical advances in the study and control of white-collar offenders. *Justice Evaluation Journal*, published online. https://doi.org/10.1080/24751979.2020.1808855

Bittle, S., & Hébert, J. (2020). Controlling corporate crimes in times of de-regulation and re-regulation. In M. L. Rorie (Ed.), *The handbook of white-collar crime* (Chapter 30, pp. 484–501). Wiley.

Bjørkelo, B., Einarsen, S., Nielsen, M. B., & Matthiesen, S. B. (2011). Silence is golden? Characteristics and experiences of self-reported whistleblowers. *European Journal of Work and Organizational Psychology, 20*(2), 206–238.

Bookman, Z. (2008). Convergences and omissions in reporting corporate and white collar crime. *DePaul Business & Commercial Law Journal, 6*, 347–392.

Borgarting. (2019, February 1). *Court case 17–170796AST-BORG/01.* Borgarting lagmannsrett (Borgarting court of appeals), judges Mats Wilhelm Ruland, Marit Bjørånesset Frogner and Bjørn E. Engstrøm. Prosecutor Esben Kyhring, defense attorney Christian Fredrik Bonnevie Hjort, Oslo, Norway.

Bowman, D., & Gilligan, G. (2008). Public awareness of corruption in Australia. *Journal of Financial Crime, 14*(4), 438–452.

Braaten, C. N., & Vaughn, M.S. (2019). Convenience theory of cryptocurrency crime: A content analysis of U.S. federal court decisions. *Deviant Behavior*, published online. https://doi.org/10.1080/01639625.2019.1706706

Brown, J. O., Hays, J., & Stuebs, M. T. (2016). Modeling accountant whistleblowing intentions: Applying the theory of planned behavior and the fraud triangle. *Accounting and the Public Interest, 16*(1), 28–56.

Bussmann, K. D., Niemeczek, A., & Vockrodt, M. (2018). Company culture and prevention of corruption in Germany, China and Russia. *European Journal of Criminology, 15*(3), 255–277.

Campagna, R. L., Dirks, K. T., Knight, A. P., Crossley, C., & Robinson, S. L. (2020). On the relation between felt trust and actual trust: Examining pathways to and implications of leader trust meta-accuracy. *Journal of Applied Psychology, 105*(9), 994–1012.

Chan, F., & Gibbs, C. (2020). Integrated theories of white-collar and corporate crime. In M. L. Rorie (Ed.), *The handbook of white-collar crime* (Chapter 13, pp. 191–208). Wiley.

Chan, J., Logan, S., & Moses, L. B. (2020). Rules in information sharing for security. *Criminology & Criminal Justice*, 1–19, published online. https://doi.org/10.1177/1748895820960199

Dearden, T. E. (2016). Trust: The unwritten cost of white-collar crime. *Journal of Financial Crime, 23*(1), 87–101.

Dion, M. (2010). Advance fee fraud letters as Machiavellian/narcissistic narratives. *International Journal of Cyber Criminology, 4*(1–2), 630–642.

Dodge, M. (2009). *Women and white-collar crime*. Prentice Hall.

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice & Research, 19*(6), 537–549.

Friedrichs, D. O., Schoultz, I., & Jordanoska, A. (2018). *Edwin H. Sutherland, Routledge key thinkers in criminology*. Routledge.

Gottschalk, P. (2017). White-collar crime: Detection and neutralization in religious organizations. *International Journal of Police Science & Management, 19*(2), 120–126.

Gottschalk, P. (2020). *Convenience dynamics and white-collar crime*. Routledge Publishing.

Gottschalk, P., & Gunnesdal, L. (2018). *White-collar crime in the shadow economy: Lack of detection, investigation, and conviction compared to social security fraud*. Springer.

Hagen, J. M., Sivertsen, T. K., & Rong, C. (2008). Protection against unauthorized access and computer crime in Norwegian enterprises. *Journal of Computer Security, 16*, 341–366.

Hamerton, C. (2020). White-collar cybercrime: Evaluating the redefinition of a criminological artifact. *Journal of Law and Criminal Justice, 8*(2), 67–79.

Hansen, L. L. (2009). Corporate financial crime: Social diagnosis and treatment. *Journal of Financial Crime, 16*(1), 28–40.

Hansen, L. L. (2020). Review of the book "convenience triangle in white-collar crime: Case studies of fraud examinations". *ChoiceConnect, 57*(5). Association of College and Research Libraries.

Harrison, A. J., Dilla, W. N., & Mennecke, B. E. (2020). Relationships within the fraud diamond: The decision processes that influence fraudulent intentions in online consumer fraud. *Journal of Information Systems, 34*(1), 61–80.

Heath, J. (2008). Business ethics and moral motivation: A criminological perspective. *Journal of Business Ethics, 83*, 595–614.

Hinduja, S. (2012). General strain, self-control, and music piracy. *International Journal of Cyber Criminology, 6*(1), 951–967.

Høyesterett. (2019). Dom avsagt 13. mai 2019 i anke over Borgarting lagmannsretts dom 23. oktober 2018 [Verdict announced May 13, 2019 regarding appeal for Borgarting court's verdict October 23, 2018]. Høyesterett (Norwegian Supreme Court).

Huff, R., Desilets, K., & Kane, J. (2010). *The national public survey on white collar crime*. National White Collar Crime Center, Fairmont. www.nw3c.org

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology, 1*(1), 1–6.

Jordanoska, A., & Schoultz, I. (2020). The discovery of white-collar crime: The legacy of Edwin Sutherland. In M. Rorie (Ed.), *The handbook of white-collar crime* (Chapter 1, pp. 3–15). Wiley.

Keil, M., Tiwana, A., Sainsbury, R., & Sneha, S. (2010). Toward a theory of whistleblowing intentions: A benefit-cost differential perspective. *Decision Sciences, 41*(4), 787–812.

Kempa, M. (2010). Combating white-collar crime in Canada: Serving victim needs and market integrity. *Journal of Financial Crime, 17*(2), 251–264.

Kim, P. H., Dirks, K. T., & Cooper, C. D. (2009). The repair of trust: A dynamic bilateral perspective and multilevel conceptualization. *Academy of Management Review, 34*(3), 401–422.

Kireenko, A. P., Nevzorova, E. N., & Fedotov, D. Y. (2019). Sector-specific characteristics of tax crime in Russia. *Journal of Tax Reform, 5*(3), 249–264.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management, 11*(4), 541–562.

Mesmer-Magnus, J. R., & Viswesvaran, C. (2005). Whistleblowing in an organization: An examination of correlates of whistleblowing intentions, actions, and retaliation. *Journal of Business Ethics, 62*(3), 266–297.

Mpho, B. (2017). Whistleblowing: What do contemporary ethical theories say? *Studies in Business and Economics, 12*(1), 19–28.

Naumovska, I., Wernicke, G., & Zajac, E. J. (2020). Last to come and last to go? The complex role of gender and ethnicity in the reputational penalties for directors linked to corporate fraud. *Academy of Management Journal, 63*(3), 881–902.

Park, H., Bjørkelo, B., & Blenkinsopp, J. (2020). External whistleblowers' experiences of workplace bullying by superiors and colleagues. *Journal of Business Ethics, 161*, 591–601.

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology, 14*(1), 1–25.

Piquero N. L., & Schoepfer A. (2010). Theories of white-collar crime and public policy. In H. D. Barlow & S. H. Decker (Eds.), *Criminology and public policy: Putting theory to work*. Temple University Press.

Podgor, E. S. (2007). The challenge of white collar sentencing. *Journal of Criminal Law and Criminology, 97*(3), 1–10.

Pontell, H. N., Black, W. K., & Geis, G. (2014). Too big to fail, too powerful to jail? On the absence of criminal prosecutions after the 2008 financial meltdown. *Crime, Law and Social Change, 61*(1), 1–13.

Pontell, H. N., Tillman, R., & Ghazi-Tehrani, A. K. (2021). In-your-face Watergate: Neutralizing government lawbreaking and the war against white-collar crime. *Crime, Law and Social Change*, 19, published online. https://doi.org/10.1007/s10611-021-09954-1

Popham, J. F., & Volpe, C. (2018). Predicting moral disengagement from the harms associated with digital music piracy: An exploratory, integrative test of digital drift and the criminal interaction order. *International Journal of Cyber Criminology, 12*(1), 133–150.

Rehg, M. T., Miceli, M. P., Near, J. P., & Scotter, J. R. V. (2009). Antecedents and outcomes of retaliation against whistleblowers: Gender differences and power relationships. *Organization Science, 19*(2), 221–240.

Sarre, R., Lau, L. Y. C., & Chang, L. Y. C. (2018). Responding to cybercrime: Current trends. *Police Practice & Research, 19*(6), 515–518.

Shawver, T., & Clements, L. H. (2019). The impact of value preferences on whistleblowing intentions of accounting professionals. *Journal of Forensic and Investigative Accounting, 11*(2), 232–247.

Stadler, W. A., Benson, M. L., & Cullen, F. T. (2013). Revisiting the special sensitivity hypothesis: The prison experience of white-collar inmates. *Justice Quarterly, 30*(6), 1090–1114.

Stone, B. (2015, March 2–March 8). Too good to be legal. *Bloomberg Businessweek*, pp. 31–33.

Sutherland, E. H. (1939). White-collar criminality. *American Sociological Review, 5*, 1–12.

Sutherland, E. H. (1983). *White collar crime—The uncut version*. Yale University Press.

Tankebe, J. (2019). Cooperation with the police against corruption: Exploring the roles of legitimacy, deterrence and collective action theories. *British Journal of Criminology, 59*, 1390–1410.

Teubner, R. A., & Stockhinger, J. (2020). Literature review: Understanding information systems strategy in the digital age. *Journal of Strategic Information Systems*, published online. https://doi.org/10.1016/j.jsis.2020.101642

Uygur, S. A. (2020). *Fraud in the charity sector in England and Wales: Accountability and stakeholder oversight*. A thesis submitted in fulfillment of the requirement for the degree of Doctor of Philosophy of Royal Holloway, University of London, United Kingdom.

Vasiu, V. I., & Podgor, E. S. (2019, July). Organizational opportunity and deviant behavior: Convenience in white-collar crime. In *Criminal Law and Criminal Justice Books*. Rutgers, The State University of New Jersey. www.clcjbooks.rutgers.edu

Walburg, C. (2020). White-collar and corporate crime: European perspectives. In M. L. Rorie (Ed.), *The handbook of white-collar crime* (Chapter 21, pp. 337–346). Wiley.

Wall-Parker, A. (2020). Measuring white collar crime. In M. L. Rorie (Ed.), *The handbook of white-collar crime* (Chapter 3, pp. 32–44). Wiley.

Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF): Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management, 19*(1), 39–53.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*(9), 1119–1131.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing & Society, 23*(4), 516–539.

2

Convenience Dimensions

Researchers have studied the explanatory power of various perspectives that might explain the likelihood and occurrence of cybercrime among white-collar offenders. Payne and Hadzhidimova (2020) reviewed such disciplinary and interdisciplinary cybercrime research and found that important general perspectives include low or lack of self-control, reaction to stress and strain, learning from others, application of neutralization techniques, and abuse of routine activities. These perspectives are important elements in the theory of convenience, where reaction to stress and strain (Hinduja, 2012; Langton & Piquero, 2007; Thaxton & Agnew, 2018) belongs in the motive dimension, routine activities (Cohen & Felson, 1979; Huisman & Erp, 2013) belong in the opportunity dimension, while self-control (Craig & Piquero, 2016; Hinduja, 2012; Holtfreter et al., 2010), learning (Leasure & Zhang, 2018; Sutherland, 1983), and neutralization (Kaptein & Helvoort, 2019; Sykes & Matza, 1957) belong in the willingness dimension of convenience theory.

The theory of convenience is an integrated and deductive perspective on white-collar offenders where individual and organizational themes interact with each other (Chan & Gibbs, 2020; Gottschalk, 2020;

P. Gottschalk and C. Hamerton, *White-Collar Crime Online*,
https://doi.org/10.1007/978-3-030-82132-6_2

Vasiu & Podgor, 2019). To integrate is to form, coordinate, or blend into a functioning or unified whole. Integration is to add perspectives and propositions that improve the validity, generalizability, and utility of a theory to explain a phenomenon and to predict potential outcomes (Fried & Slowik, 2004; Hambrick & Lovelace, 2018).

The theory of convenience integrates various perspectives on convenience into a single theory with greater comprehensiveness and explanatory value than any one of its component perspectives. As such, convenience theory attempts to explain white-collar crime by bringing together several different theories and invoking multiple levels of analysis at the individual, organizational, as well as societal levels as suggested by Friedrichs (2010: 479):

> The number of different theories or levels, and the formality, with which the relationship between the theories or variables on different levels of analysis is posited, varies.

Convenience theory explains white-collar offenders' financial motives, organizational opportunities, and personal willingness for deviant behaviors.

Convenience in Financial Motive

It is convenient to use illegitimate financial gain to explore possibilities and avoid threats. Climb the hierarchy of needs for status and success (Maslow, 1943), realize the American dream of prosperity (Schoepfer & Piquero, 2006), satisfy the need for acclaim as a narcissist (Chatterjee & Pollock, 2017), and restore the perception of equity and equality (Leigh et al., 2010) are some of the perspectives integrated in the motive dimension of convenience theory. In addition, goal setting is a common practice in the field of organizational behavior, where high performance goals tend to encourage unethical behavior (Welsh et al., 2019). The extra profit from financial crime enables the offender to handle desired possibilities and potential threats. It is mainly the convenience of extra

profit, rather than the convenience of illegal profit, that is important in the motive dimension of convenience theory.

However, under certain circumstances, there might be some extra benefits from illegal extra profit rather than extra profit in general, since illegal funds avoid the attention of external and internal control mechanisms, including compliance functions (Kawasaki, 2020). Illegitimate financial gain can thus find its ways into exploring possibilities and avoiding threats that recorded funds cannot. It has been argued that convenience does not provide a motive and thus does not make someone want to climb the hierarchy of needs. However, illegitimate gain is a strong motive to do what you otherwise would not have done, where convenience can be found in the use of illegal gain.

White-collar offenders online can explore the special benefits from illegal gain as the money might be transferred on digital networks according to financial motives that are unattainable for legal gain. If the motive is to have money placed in tax havens, commit corruption, receive bribes, finance terrorism, or has other purposes for which many nations have control mechanisms, then it is more convenient in the motive dimension to have money from fraud and other forms of financial crime than from regular and legal business practices. A financial motive thus becomes relevant for offenders online.

Some white-collar offenders have the financial motive of reaching business objectives that justify means (Jonnergård et al., 2010), satisfying the desire to help others as social concern (Agnew, 2014), satisfying greed where nothing is ever enough (Goldstraw-White, 2012), avoiding corporate collapse and bankruptcy (Kang & Thosuwanchot, 2017), or enjoying mutual benefits in exchange relationships (Huang & Knight, 2017). Some offenders have the motive of avoiding loss of self-esteem after organizational failure (Crosina & Pratt, 2019), removing strain, pain, and uncertainty (Hinduja, 2012; Langton & Piquero, 2007), avoiding falling from position in the privileged elite (Piquero, 2012), adapting to profitable criminal market forces (Schoultz & Flyghed, 2020a, 2020b, 2021), or joining profitable criminal networks (Goncharov & Peter, 2019).

Greed is the most acknowledged motive for financial crime by white-collar offenders. Goldstraw-White (2012) defines greed as socially

constructed needs and desires that can never be completely covered or contended. Greed can be a very strong quest to get more and more of something, and there is a strong preference to maximize wealth. To outsiders it may seem strange that rich people have such a strong desire to become even richer that they are willing to break the law. However, as the definition indicates, greedy individuals are never happy with what they have, as they desperately want more all the time. Prosperity is not a means, but a goal for greedy individuals. Greed can grow when the organization does not have an adequate reaction (Haynes et al., 2015). Greed is a typical motive for occupational crime where individuals enrich themselves. Greed implies that some people never become satisfied with what they earn or what they own. There is a lack of satisfaction with whatever one has. Greed can be a strong quest to maximize wealth as wealth is also a symbol of success. Greed leads to a need for an increasingly larger home, several chalets, and summerhouses, bigger boat, luxurious vacations, and ownership in various enterprises. Greed is a desire among all sorts of people. When there are simple possibilities for financial gain to enjoy prosperity, then economic crime can be a convenient action. Both Bucy et al. (2008) and Hamilton and Micklethwait (2006) emphasize greed as the most common cause of criminal acts by white-collar offenders.

In many organizations, ends justify means (Campbell & Göritz, 2014). If ends in terms of ambitions and goals are difficult to realize and achieve in legal ways, illegal means represent an alternative in many organizations (Jonnergård et al., 2010). Among most executives, it is an obvious necessity to achieve goals and objectives, while it is an obvious catastrophe failing to achieve goals and objectives. Welsh and Ordonez (2014) found that high performance goals cause unethical behavior.

Convenience in Professional Opportunity

There is convenient access to resources to commit and conceal financial crime. Legitimate access to premises and systems (Benson & Simpson, 2018), specialized access in routine activity (Cohen & Felson, 1979), blame game by misleading attribution to others (Eberly et al., 2011),

and institutional deterioration (Rodriguez et al., 2005) are some of the perspectives integrated in the opportunity dimension of convenience theory. A typical white-collar offender does not go into hiding as many street criminals do. Rather, the offender conceals financial crime among legal transactions to make illegal transactions seem legitimate, or the offender conceals financial crime by removing certain activities from the books. A typical white-collar offender who has convenient legitimate access to commit crime might spend most of the energy on concealing crime in the professional context.

White-collar offenders offline can use executive language that people do not understand (Ferraro et al., 2005), while white-collar offenders online can use digital techniques that people do not understand. Misleading attribution to others is possible in the digital space, where email addresses and webpage labels can attribute deviant behavior and thus blame to others (Resodihardjo et al., 2015). Offender humor can distract from deviant behavior by application of various digital symbols online (Yam et al., 2018). There is power inequality between the elite and others (Patel & Cooper, 2014), where offenders online can pretend to have the necessary authority.

Since offenders have legitimate access to their own premises and systems (Benson & Simpson, 2018), they have the opportunity to exploit their legitimate access to move electronically into other digital spaces. Opportunity creation by entrepreneurship is indeed possible (Ramoglou & Tsang, 2016), where the entrepreneurial effort online is concentrated on both committing and concealing crime. Offenders may have convenient specialized access in routine activity (Cohen & Felson, 1979) and legitimate access to strategic resources in terms of digital tools and techniques (Adler & Kwon, 2002). Scheaf and Wood (2021: 2) found that entrepreneurial fraud has stimulated a wide array of research related to white-collar crime, where they provided the following definition of entrepreneurial fraud:

> Enterprising individuals (alone or in groups) deceiving stakeholders by sharing statements about their identity, individual capabilities, elements of new market offerings, and/or new venture activities that they know to be false in order to obtain something of value.

While the common understanding of entrepreneurship is focused on the positive and productive aspects, entrepreneurial fraud focuses on the dark aspects. It is all about deception used to obtain valuable resources from stakeholders (Scheaf & Wood, 2021).

An important element of the opportunity structure is deterioration in computer systems lacking technical guardianship and lacking supervising competence from absence of technology expertise. A consequence is institutional deterioration (Rodriguez et al., 2005), where nobody feels responsible for whatever goes on in computer systems. There is an inability to control because of social disorganization (Hoffmann, 2002), where online activities are neither coordinated nor reviewed.

The lack of information technology competence in the organization makes it difficult—if not impossible—to distinguish between digital noise and digital crime signals (Karim & Siegel, 1998; Szalma & Hancock, 2013). While executives are spending their working days in meeting rooms talking, technology employees try to fix digital issues when often failing to communicate with others. There is thus a failure of coordination in the principal–agent relationship between executives and experts (Bosse & Phillips, 2016). It is often extremely difficult for outsiders to make sense of what is going on in computer systems (Holt & Cornelissen, 2014; Weick et al., 2005). Computer systems tend to be considered as black box, where people only understand what goes into systems and what comes out of systems, while being unable to understand what happens inside the systems. People thus fail in sense making, where sense making is the process of creating meaning through interpretation of cues (Hällgren et al., 2020). Surprisingly often, people trust computer systems although they are unable to make sense of what is going on inside them.

Even when someone notices deviance and potential wrongdoing, most people are reluctant to blow the whistle and notify relevant entities. It is well-known that whistleblowers often experience retaliation and reprisals without any benefits from whistleblowing for themselves (Bjørkelo et al., 2011; Keil et al., 2010). In addition, there can be an ethical climate conflict (Victor & Cullen, 1998), which strengthens the opportunity structure for offenders.

Convenience in Behavioral Willingness

White-collar offenders online can conveniently justify crime and neutralize potential guilt feelings. By neutralizing guilt feelings, offenders do not feel accountable, ashamed, or responsible (Chen & Moosmayer, 2020). Application of neutralization techniques (Sykes & Matza, 1957), sliding on the slippery slope (Welsh et al., 2014), lack of self-control (Gottfredson & Hirschi, 1990; Hinduja, 2012), narcissistic identification with the organization (Galvin et al., 2015), learning from others by differential association (Sutherland, 1983), and professional deviant identity (Obodaru, 2017) are some of the perspectives integrated in the willingness dimension of convenience theory. When a white-collar offender justifies crime, then it is obvious to him or her that wrongdoing occurred. However, the offender can claim that the act of wrongdoing is morally justifiable (Schnatterly et al., 2018), and that a negative life event has occurred and is to blame (Engdahl, 2013). When a white-collar offender denies a guilty mind, then the offender applies neutralization techniques (Kaptein & Helvoort, 2019; Whyte, 2016). When a white-collar offender makes crime as a choice, it is convenient based on identity (Galvin et al., 2015), rationality (Pratt & Cullen, 2005), and learning from others (Sutherland, 1983). Convenience in behavior refers to convenience of the rationalizations, excuses, and neutralizations.

White-collar offenders online can have a professional deviant identity (Obodaru, 2017). The identity perspective suggests that individuals develop professional identities where they commit to a chosen identity. It is a process of generating possible selves, selecting one, and discarding others. Professional identity is how an individual sees himself or herself in relation to work. The self-concept is a complex cognitive structure containing all of a person's and possibly an organization's self-representations (Cloutier & Ravasi, 2020; Graham et al., 2020). An online offender can have a self-concept of a technology expert, where victims are considered losers incapable of protecting themselves. According to the identity perspective, roles and identities are interdependent concepts. Identity enactment refers to acting out an identity or claiming the identity by engaging in behaviors that conform to role expectations and that allow the identity to become manifest. Deviant

behavior finds an anchor in a person's professional identity (Crank, 2018), where the deviant leader must claim and assume a leader identity by their followers.

Labeling can influence the deviant personality offender mind (Mingus & Burchfield, 2012). The labeling perspective suggests that individuals adapt to the reputation created by others (Crank, 2018). A white-collar offender online might act according to the label of a technology expert, where the limits are not whether or not an act is illegal, but rather whether or not an act is technologically feasible to commit and conceal. The labeling perspective argues that the deviant reputation stigmatizes a person into a stereotype. Formal societal reaction to the individual can be a stepping-stone in the development of a criminal career. The deviant label is over time embedded in the individual. The labeled person is increasingly likely to become involved in social groups that consist of social deviants and unconventional others without feeling any doubt or regret since the behavior is in accordance with the label glued to the person by others (Bernburg et al., 2006).

The choice of crime might derive from sensation seeking. Craig and Piquero (2017) suggest that the willingness to commit financial crime by some white-collar offenders has to do with their inclination for adventure and excitement. Offenders are not only seeking new, intense, and complicated experiences and sensations, as well as exciting adventures, they are also accepting the legal, physical, financial, and social risks associated with these adventures. They attempt to avoid boredom by replacing repetitive activities such as regular meetings with thrill and adventures. They search risky and exciting activities and have distaste for monotonous situations. A white-collar offender online can experience new, intense, and complicated adventure, sensation, and excitement when attacking internal and external digital networks and systems for illegitimate financial gain.

White-collar offenders can take on professional deviant identities depending on the space where activities take place. As suggested by Al-Suwaidi et al. (2018), people behave differently when they move from one space to another. For example, in email communication, people tend to have an overemphasis on the sender role rather than the receiver role as compared to face-to-face interaction. In the digital space it can