Let the buyer beware: how network structure can enable (and prevent) supply chain fraud

Scott DuHadway and Carlos Mena
School of Business, Portland State University, Portland, Oregon, USA, and
Lisa Marie Ellram
Management, Farmer School of Business, Miami University, Oxford, Ohio, USA

Received 24 May 2021
Revised 10 November 2021
Accepted 19 November 2021

Abstract

Purpose – Supply chain fraud is a significant global concern for firms, consumers and governments. Evidence of major fraud events suggests the role of supply chain structures in enabling and facilitating fraud, as they often involve several parties in complicated networks designed to obfuscate the fraud. This paper identifies how the structural characteristics of supply chains can play an important role in enabling, facilitating and preventing fraud.

Design/methodology/approach – The research follows a theory elaboration approach. The authors build on structural holes theory in conjunction with a multiple case study research design to identify new concepts and develop propositions regarding the role of network structure on supply chain fraud.

Findings – This research shows how structural holes in a supply chain can create advantages for unscrupulous firms, a role we call tertius fraudans, or the cheating third. This situation is exacerbated by structural ignorance, which refers to the lack of knowledge about structural connections in the network. Both structural holes and structural ignorance can create information gaps that facilitate fraud, and the authors propose solutions to detect and prevent this kind of fraud.

Originality/value – This paper extends structural holes theory into the domain of fraud. Novel concepts including tertius fraudans, structural ignorance and bridge collapse are offered, alongside a series of propositions that can help understand and manage structural supply chain fraud.

Keywords Opportunism, Fraud, Structural holes theory, Case study research

Paper type Research paper

Introduction

As supply chains face increasing pressures, some firms make the choice to engage in fraudulent practices. This has become increasingly relevant as the coronavirus disease 2019 (COVID-19) pandemic has created mismatches between supply and demand, producing incentives to engage in fraud. As early as June 2020, the European Anti-Fraud Office identified 340 companies selling counterfeit or substandard products linked to the COVID-19 pandemic, and cases of counterfeit medical supplies, test kits and other goods have been reported by Interpol (2020), US Customs and Border Protection (2020), the World Customs Organization (2020) and the Center for Disease Control and Prevention (2021).

Although structural supply chain fraud has an obvious negative impact, research capturing the total cost of this type of fraud remains limited. Of such evidence, the total cost of fraud has been estimated to be as much as 5% (Association of Certified Fraud Examiners, 2016) to 9% of the annual revenues of a typical firm (DuHadway *et al.*, 2020). For this research, we define supply chain fraud as *an unlawful act of deception through omission or commission perpetrated by one or more actors in a supply chain leading to harm for other actors in the supply chain.* This encompasses a variety of different frauds, for example, product quality fraud, invoicing fraud, data fabrication, counterfeit manufacturing and unauthorized production. Supply chain fraud has been identified as critical in industry publications, with some reports calling it the "most exposed area" of fraud (KPMG, 2010, p. 3). Arguably, a great deal of research exists about fraud within organizational boundaries and even among dyads

International Journal of Operations & Production Management
© Emerald Publishing Limited
0144-3577
DOI 10.1108/IJOPM-05-2021-0310

of organizations. Yet, there is limited research exploring supply chain fraud–and little consensus on how to address it.

Many notable examples of fraud involve multiple supply chain actors, for instance, the Mattel recalls for lead-based paint in children's toys (Kavilanz, 2009), the horsemeat scandal (Lawrence, 2013) and the Takata airbag recalls (Ivory and Tabuchi, 2015). These examples demonstrate that structural supply chain fraud is a network-level phenomenon, as the adverse outcomes of fraud were enabled and magnified by the structure of the supply chain.

We contend that structural supply chain fraud has been the subject of limited research for three reasons. First, research on fraud is difficult because the phenomenon is covert, often because it is not in the interest of any actors to reveal it. Even victims can have concerns about the negative exposure and thus conceal the fraud. This restricts access to data and limits methodological choices. Second, limited previous research on supply chain fraud restricts the theoretical basis from which to establish future research on fraud, making future research riskier and more difficult. Third, fraud in a supply chain context has not been precisely defined due to overlaps with several other fields of research (e.g. accounting, finance and criminology) and several supply chain topics (e.g. opportunism, corruption and risk), creating divergent research streams with different foundational backgrounds.

We seek to address these challenges by developing a definition of structural supply chain fraud, presenting a theoretical basis for exploring structural supply chain fraud and establishing a valuable framework to investigate structural supply chain fraud. Specifically, this paper aims to illuminate how supply chain structure enables and facilitates fraud. This research extends the previous work on antecedents and drivers of fraud by considering the structural relationships between organizations and how structure can enable and prevent fraud.

The rest of the research paper is structured as follows: First, we provide a background and define the phenomenon of structural supply chain fraud. We then discuss the theoretical lenses that can help explain the phenomenon. This is followed by the methodology section where we describe our research approach and data collection and analysis methods. The theory elaboration section brings together structural holes theory with the empirical evidence to theorize about structural supply chain fraud. Here we identify emerging constructs, and present propositions that help explain structural supply chain fraud and provide insights on how to prevent it. Finally, we present the conclusions, limitations and opportunities for further research.

Background

Before delving into the conceptualization of structural supply chain fraud, we discuss a related concept that appears extensively in the literature: opportunism. The concept of opportunism figures prominently in theories used to explain inter-organizational behavior (Wathne and Heide, 2000), most notably, TCE (Williamson, 1975) and agency theory (Eisenhardt, 1989; Jensen and Meckling, 1976). Opportunism, defined as "self-interest seeking with guile" (Williamson, 1975, p. 6), is at the core of the principal-agent problem, which occurs when a buyer (i.e. principal) delegates a task to a supplier (i.e. agent), and difficulties exist in verifying whether the supplier is acting in the buyer's best interest (Eisenhardt, 1989; Jensen and Meckling, 1976). This agency problem is exacerbated by goal incongruence and information asymmetries (Jensen and Meckling, 1976), likely antecedents of fraudulent behavior.

Conceptualizations of opportunism tend to frame it as a dyadic governance problem, where one member of the dyad acts in self-interest without considering the other. In line with this framing, most proposed solutions to opportunism focus on governance mechanisms, which can come in contractual and relational forms (Lee and Cavusgil, 2006; Macneil, 1978). Contractual mechanisms are formal, legally-binding agreements that document promises and obligations (Um and Oh, 2020; Lee and Cavusgil, 2006; Macneil, 1978). Relational mechanisms are informal

and emerge from the values and processes developed in the relationship, including norms such as trust, flexibility, solidarity and information exchange (Fulmer and Gelfand, 2012; Pilbeam *et al.*, 2012; Poppo and Zenger, 2002). While both contractual and relational mechanisms are important for constraining opportunism, they are limited in their focus on the dyad, overlooking the structural aspects that can allow or prevent opportunistic behavior.

Corruption is another topic that is related to the both opportunism and fraud, and consists of a wide range of behaviors and sometimes includes various types of fraud (Rose-Ackermann and Palifka, 2016; Silvestre *et al.*, 2020). As Arnold *et al.* (2012, p. 138) note: "Corruption can have many forms. Examples of corruption include bribery (soliciting, offering or accepting a bribe) of or by public officials, bribery in the private sector, conflict of interest, fraud, money laundering and trading in influence. (p. 138)". Given the broad range of behaviors that can be classified under opportunism or corruption, we next define supply chain fraud which is the focus of this paper.

Adequately defining fraud is a challenge that dates back centuries; as Stephen (1883, p. 28) notes in the late 1800s, "The difficulty of giving an adequate definition of fraud has been felt at all times." Legal definitions vary by jurisdiction, and academic definitions exhibit a similar degree of variance by academic disciplines. To craft our definition of supply chain fraud, we follow Hempel's (1970, p. 654) advice that a "good" formal, conceptual definition should be inclusive, exclusive, differentiable, clear, communicable, consistent, and parsimonious (Hempel, 1970, p. 654) and apply these general principles to existing definitions from different domains. We then seek commonalities and differences across these definitions and select properties relevant to a supply chain domain to define its boundaries. Table 1 presents a selection of definitions of fraud from different perspectives.

Consistent among the various definitions are three key elements. First, they all involve at least two actors, the perpetrator, who commits the fraudulent act and the victim, who is affected by it. However, some definitions acknowledge that there could be multiple perpetrators and multiple victims. Second, fraud involves a dishonest or deceitful act that is unlawful. Third, the fraudulent act leads to harm for the victim(s), which can include economic losses, operational disruptions, reputation loss, consumer harm and risk exposure through compliance violations (KPMG, 2017).

The definitions in Table 1 also show differences in terms of the unit of analysis and intention of the actors. In terms of unit of analysis, definitions may refer to individuals, groups or organizations. For this research, we seek a definition that operates at an organizational level. In terms of intention, some definitions focus on intentional acts or acts of commission, and others also include acts of inaction or negligence, this is, acts of omission. Here we opt for a more comprehensive approach. Building on the previous definitions, we define supply chain fraud *as an unlawful act of deception through omission or commission perpetrated by one or more actors in a supply chain leading to harm for other actors in the supply chain.*

It is important to note that our definition incorporates the possibility of a fraudulent act being perpetrated by multiple actors, some of which commit the act as perpetrators (e.g. a manufacturer of a counterfeit product), and some that could be involved by omission, simply casting a blind eye or failing to act in the face of a fraudulent act (e.g. a distributor not acting on suspicions of possible counterfeit products). Similarly, the definition incorporates the possibility of multiple victims. One such example is a retailer buying an unknowingly adulterated product that is then sold to a consumer. In this event, though the degree and type of harm might differ for the retailer and the consumer, both are victims of fraud. While supply chain fraud can occur at a dyadic level, in this research, we are interested in a type of fraud in which structure plays a role through the creation of blind spots, which can be exploited by malicious actors.

Fraud exists as a particularly extreme form of opportunistic behavior, and traditional controls to limit opportunism might fail when it comes to risks from intentional actions such

Definition	Context	Source
Criminal deception; the using of false representations to obtain an unjust advantage or to injure the rights or interests of another	Dictionary	Oxford English Dictionary
An individual or an organization intentionally makes an untrue representation about an important fact or event; the untrue representation is believed by the victim (the person or organization to whom the representation has been made); the victim relies upon and acts upon the untrue representation; the victim suffers loss of money and/or property as a result of relying upon and acting upon the untrue representation	Accounting	Simmons (1995)
1) a party is (severely) damaged, as a result of 2) deception by some other party	Interorganizational	Firozabadi *et al.* (1998, p. 278)
First, deceit or an intention to deceive or in some cases mere secrecy; and, secondly, either actual injury or possible injury or an intent to expose some person either to actual injury or to a risk of possible injury of that deceit or secrecy	Legal	Stephen (1883, p. 121)
In legal terms, fraud is a generic category of criminal conduct that involves the use of dishonest or deceitful means in order to obtain some unjust advantage or gain over another In business terms, fraud is sometimes difficult to define as it extends, for example, from conduct as trivial as an employee having an extended lunch break without permission, to large-scale misappropriation of funds by a company accountant involving many millions of dollars	Business and legal	Smith (2001, p. 1–2)
Acts of omission or commission by individuals or groups of individuals, acting in their organization roles, who violate internal rules, laws or administrative regulations on behalf of organizational goals. The extent of adverse consequences and harm to the public will vary with the act, so social cost may be contained or diffused	Interorganizational (definition for misconduct)	Vaughan (1999, p. 288)
A deliberate act that is contrary to law, rule, or policy with intent to obtain unauthorized financial benefit.	Financial fraud	Ngai *et al.* (2011, p. 559)

Table 1.
Definitions of fraud from different domains

as fraud (DuHadway *et al.*, 2019). Opportunism is viewed as a "fundamental assumption about firm behavior" (Li and Choi, 2009, p. 34), suggesting that it is both expected and falls within traditional assumptions about firm relationships. In contrast, fraud exists outside the normal rules of engagement as organizations perpetrating fraud are not bound by conventional constraints or rules of engagement. For example, fraudulent firms may knowingly falsify data, violate contracts and engage in unlawful acts–many of which are assumed to be sacrosanct in interorganizational relationships.

Theoretical positioning

Researchers emphasizing the interorganizational context of fraud have primarily relied on the dyadic perspective considering the relationship and oversight between two firms. Theories such as transaction cost economics (TCE) (see Lumineau and Oliveira, 2020 for a recent review)

and agency theory (AT) (e.g. Eisenhardt, 1989; Shevchenko *et al.*, 2020), where opportunistic behavior figures prominently, have traditionally been used to explain and predict opportunism in supply chains. TCE explains how information asymmetries can create conditions favorable to firms to engage in self-interest seeking with guile (Williamson, 1975). Similarly, AT predicts that agents are more likely to engage in opportunistic behavior when it is difficult for principals to monitor their behavior (Eisenhardt, 1989; Sharma, 1997). However, these theories focus predominantly on dyadic relationships, downplaying structural aspects. AT has been extended across multiple tiers, a phenomenon known as double agency (Wilhelm *et al.*, 2016) or multiple agency (Arthus *et al.*, 2008). However, these extensions have not focused on structural issues, but rather on the conflicts of interest between multiple parties, and the possible solutions to such conflicts (Arthus *et al.*, 2008; Child and Rorigues, 2003).

Social network theory (Freeman, 1979; Freemen *et al.*, 1992) focuses on the structural aspects of the network but ignores opportunism, constraining the applicability of the theory in the context of fraud. The theory of network governance (Jones *et al.*, 1997) combines elements of social network theory with TCE and accounts for both opportunism and structure, providing safeguards against opportunism based on social mechanisms. However, it does not offer explanations about how the structure of the network affects opportunism. Similarly, institutional theory (DiMaggio and Powell, 1983; Oliver, 1991) contemplates how the mechanisms of institutional isomorphic change (coercive, normative, mimetic) can curb opportunism, but does not illuminate the relationship between structure and opportunism. Research exploring the role of corruption in operations and supply chain management identifies that "fraud is more of a structural issue than a personal issue." (Arnold *et al.*, 2012, p. 143), emphasizing that it is the circumstances that create opportunities for fraud that should be investigated.

Structural holes theory (Burt, 1992, 2002, 2004) is based on the notion that the absence of ties between firms (i.e. structural holes) create brokerage opportunities that can enhance performance for those network members prepared to exploit these holes (Burt, 1992). In essence, structural holes theory explains how firms can take advantage of their position in the network. While this explanation does not explicitly deal with fraud, the theory appears to be better suited to go beyond the dyad, while providing a plausible explanation for the role of structure in opportunistic behavior. As Choi and Wu (2009) submit, the smallest unit of analysis in a network is not a dyad, but a triad, because a triad allows us to examine how a node affects another node and how a link affects another link. Thus, we argue that structural holes theory provides the necessary building blocks to construct a theory of structural supply chain fraud.

Table 2 presents a comparison of theories that are relevant either to phenomena associated with opportunism (and fraud) or to the structure of networks.

Methodology

Our inquiry aims to explain the phenomenon of structural supply chain fraud. Given that this phenomenon remains largely unexplored in the literature, we decided to follow a theory elaboration approach. This approach applies an existing general theory in a relatively unexplored context, where not enough is known to formulate detailed hypotheses for testing (Ketokivi and Choi, 2014). Instead, empirical evidence is used to challenge and extend theory (Ketokivi and Choi, 2014; Voss *et al.*, 2002).

Ketokivi and Choi (2014) describe the aim of theory elaboration as a reconciliation of the general (i.e. the theoretical) with the particular (i.e. the empirical). In this research, the theoretical grounding rests on structural holes theory because it provides a structural explanation for opportunistic behavior and caters to networks of three or more actors. The empirical grounding of the research rests on a multiple-case research design that follows a logic of literal replication (Yin, 2009; Eisenhardt, 1989; Voss *et al.*, 2002). Through the case studies, we sought to garner

Table 2. Synthesis of possible theoretical explanations for structural supply chain fraud

Theory	Social networks	Theory of network governance	Institutional theory	Structural holes theory	Transaction cost theory	Agency theory
Unit of analysis	Network	Network	Social structure	Triad and network	Dyad	Dyad (focus on principal)
Core concepts	Node size Density Centrality Link strength	Demand uncertainty Task complexity Human asset specificity Frequency Structural embeddedness Social mechanisms (i.e. restricted access, macroculture collective sanctions, and reputation)	-Isomorphism -Mechanisms of institutional isomorphism: coercive, normative, mimetic	Structural hole *Tertius gaudens* *Tertius iungens* Bridge	Coordination costs Transaction risk Coordination costs Operational risk *Opportunism risk* Asset specificity Uncertainty Bounded rationality	*Information asymmetry* Self-interest Bounded rationality Risk aversion Moral hazard Trust Contract
Structural considerations	The structure of nodes and ties that link them is central to the behavior of the network	Networks are governed by structural embeddedness, which allows firms to use social mechanisms to safeguard exchanges	Institutions (including networks) are governed by mechanisms of structural isomorphism	Holes in the network provide opportunities but also expose firms to opportunism	Firms decide between hierarchy and market	Limited. Only when considering double agency
Role of opportunism, corruption and fraud	N/A	Opportunism can be safeguarded through *social mechanisms*	Opportunism curbed by mechanisms: -*Coercive*: Legally sanctioned through rules and laws -*Normative*: Morally governed through certifications, etc. -*Mimetic*: Culturally supported through schema	*Tertius gaudens* takes an opportunistic role Firms can safeguard by *removing the bridge*	Opportunism creates risks, and firms should safeguard against it (through *contracts* and governance strategies)	The agency problem is a problem of opportunism. The principal seeks mechanisms, such as *contracts*, to safeguard against it
Main sources	Freeman (1979); Freemen *et al.* (1992)	Jones *et al.* (1997)	DiMaggio and Powell (1983); Oliver (1991); Selznick (1948)	Burt (1992, 2002, 2004); Zaheer and Bell (2005); Li and Choi (2009)	Coase (1937); Williamson (1975, 1985)	Eisenhardt (1985, 1989), Jensen and Mekling (1976)

evidence to extend and give shape to the theoretical explanations of structural supply chain fraud. Figure 1 presents a graphical depiction of the theory elaboration process, showing how the research emerged from the interplay between theory and practices, and continued through the reconciliation of theoretical foundations and empirical evidence.

Case study selection

The unit of analysis in this research is the network because structural supply chain fraud is a network-level phenomenon. Thus, our primary selection criteria were the presence of fraud and the involvement of three or more actors, including perpetrators, enablers and victims. Given the covert nature of fraud, an additional criterion became the availability of data to allow the investigation of the actors, their roles and the structure of the network.

Five retrospective case studies were conducted in two waves, as depicted in Figure 1. The first wave involved identifying historical cases that were already well-documented. Three cases stood out due to their scale and the involvement of large multinationals: the Mattel lead paint contamination scandal, the horse-meat scandal in Europe and the Takata airbag recalls. These cases present evidence of fraud involving multiple actors and the existence of publicly available data. Although these cases occurred in different timeframes, industries and geographies, they also shared several commonalities. First, they involved fraudulent actions that resulted in large-scale product recalls. Second, both involved multiple organizations playing different roles in the fraud. Third, the structural relationships among network participants appeared to play a role in the fraud. Finally, both cases revealed network structures including perpetrator(s), enabler(s) and victim(s).

For the second wave of cases, we followed a more structured approach, seeking legal cases involving fraud, and using legal documents as the primary source of data. These cases provide a documented account of the events and interactions between firms that led to fraud, including the actions of the perpetrator(s) and the harms suffered by the victim(s). To identify suitable cases for the second wave, we used two publicly available databases: LexisUni and Justice.gov. LexisUni is a legal database that covers cases filed in state and federal courts in the United States, as reported by the US Justice Department. To establish a nomological net, we searched both databases for evidence of counterfeit manufacturing during the most recent available year of 2019.

To identify cases in the second wave, we used the search string "counterfeit fraud supplier manufact* contract." These terms were selected to find counterfeiting cases that emphasized the supply chain manufacturing context and involved organizations with established relationships. The search resulted in 60 cases. We then applied three filtering criteria: (1) cases contained specific information about the counterfeit products, (2) cases involved three or more supply chain members, not including final customers, and (3) the case contained objective information sufficient to explain the process. Using these criteria, we selected two additional cases. One was based on the unauthorized resale of faulty FitBit products, and one on the sourcing of counterfeit lenses by resellers of Maui Jim glasses.

Table 3 presents a summary of the five case studies, including information about the perpetrators, victims and enablers, as well as the structural characteristics of the networks.

Data collection

Collecting data about fraud is difficult because the perpetrators exploit information asymmetries, and hide information to protect their position. Moreover, when a firm is actively involved in fraud, it is often the case that few employees are aware of it, so finding key informants can be challenging. For victims of fraud, there is also limited interest in bringing the case to light unless they are seeking restitution from the perpetrator through legal means. This creates challenges for data collection.

Figure 1.
Overview of the theory elaboration process

Case	Mattel	Horse meat	Takata	FitBit	Maui Jim
Context	Toy manufacturing in China	Food production in Europe	Airbag manufacturing worldwide	Unauthorized sell of scrap products in USA	Unauthorized resell of products outside of the approved supply chain
Timeframe	2007	2012	1995–2013	2017	2016–2019
Fraud actions	Using an unapproved supplier; circumventing required testing protocol	Horsemeat relabeled and sold as beef; using an unapproved supplier	Deleting data; information hiding	Selling unauthorized scrap products as legitimate; counterfeit packaging	Selling products to an unapproved supply chain Products sold as legitimate, with different components
Perpetrator(s) or Enabler(s)	Lee Der Donxing Zhong Xin Colorants	Comigel, Spanghero, Draap, APB food Group (Silvercrest)	Takata, Honda	BCS, Cali Resources, Laguna 2	SBG, authorized distributor, alternative lens supplier
Victim(s)	Children, Mattel	Consumers, grocers	Vehicle Owners	Consumers, Fitbit	Maui Jim, consumer
Other roles	Other approved paint suppliers	Doly com, horsemeat supplier	Autoliv, as a comparison to Takata's actions	Groupon facilitated the sell, but likely unaware of the product being designated scrap	Alternative lens supplier is knowingly or unknowingly involved in the fraud
Outcomes	Major recalls, process-based changes and increased oversight	Major recalls, supply chain restructuring	Largest automotive recall in history, many deaths and injuries	Legal case seeking injunction to ban further sell of products	Costs < $10k and terminated relationship with authorized distributor
Structural characteristics	Structural links were unknown and outside of approved lists	Highly complex, multiple transactional layers for simple product flow, many structural holes	Relatively simple, Takata – > Honda – > consumers, with information hidden across each structural hole	Highly complex with multiple transactional layers. Hidden supply network, network was hidden by perpetrators	Relatively simple, with a fraudulent supply chain alongside the traditional supply chain

(*continued*)

Table 3.
Case study summary

Case	Mattel	Horse meat	Takata	FitBit	Maui Jim
Other notable characteristics	High degree of contractual governance and monitoring systems, but assumed the rules would be followed	Significant blaming of other parties, always pointing upstream	The situation seemed to continue to get worse over time, with no viable exit. The only way forward was to keep doing more fraud	Refusal to disclose supply network	The network had a double bridge, and extending the supply chain undermined contractual governance controls. Refusal to disclose supply network
Data sources	House hearing, case studies, Media reports	Media reports, House of commons report, testimony of executives, European commission	Senate report, Media reports, Internal emails	Fitbit, Inc. v. Laguna 2, LLC, 2017	Maui Jim, Inc. v. Smartbuy Guru Enterprises., 2017
Motivation	Lack of product availability, avoiding production Delays	High industry pressure, $$	Company viability, $$	Access to cheaper products, $$, lack of adequate oversight	Access to product, $$

Table 3.

Given the data collection constraints associated with this phenomenon, we relied exclusively on secondary sources, similar to previous work investigating corruption which faces similar challenges (Silvestre *et al.*, 2020). Furthermore, data usually becomes available after the fraud has been exposed, so the data are retrospective. However, since fraud cases often extend over a period of time, the retrospective data provides insights on not only how the fraud was conducted but also how it was exposed and how it concluded.

Given the secondary nature of the data, it is important to verify the integrity of the data. In order to do this, we used triangulation across many different sources, including statements and testimonies made to government bodies, in-depth detailed investigations and legal cases. This approach allowed us to compare key features of these cases and draw inferences to develop our research with a greater degree of reliability.

Case study analysis

The case studies were analyzed using a qualitative data analysis approach based on Miles and Huberman (1994), which follows an iterative process involving data collection, data reduction, data display, and conclusion formulation and verification. At this stage, theorizing is grounded on both the concepts of structural holes theory and the data collected in our cases. This allowed us to elaborate on structural holes theory by proposing extensions to the original constructs and some new constructs relevant to this investigation. This process led to formulating a series of propositions concerning the structural and governance conditions that enable and facilitate structural supply chain fraud.

First, we conducted a within-case analysis where we collated and analyzed each case, creating a structural map of the actors involved, understanding the role of each of the actors

and identifying the contextual factors influencing each case. Appendix 1 provides synthesized narratives based on the within-case analysis. Second, we conducted a cross-case analysis where we compared and contrasted the findings of the five case studies, seeking to establish consistencies and inconsistences with the theoretical explanations of structural holes theory. The results of these comparisons lead to extensions of structural holes theory in the context of fraud.

Theory elaboration

We elaborate on structural holes theory by incorporating current practice and proposing how structure can facilitate fraud. First, we present new concepts associated with structural holes theory that emerged from our analysis. Then, we articulate propositions theorizing about how the structural characteristics of a supply chain can create opportunities for fraud, and offer opportunities for concealing fraud. Conversely, structural characteristics can also help to prevent or at least constrain fraudulent behavior. For each set of propositions presented below, we begin by providing a theoretical foundation. Then, we present the theoretical elaboration, incorporating empirical evidence into the theoretical foundation. We then present a set of propositions formulated based on both theoretical and empirical underpinnings. Finally, we discuss divergent themes identified from the cases, which could emerge as avenues for future research.

Theoretical foundation: the constructs of structural holes theory

Burt (1992) argues that firms can gain competitive advantage by designing networks that maximize disconnections (or structural holes) between network actors. A *structural hole* refers to a separation between nonredundant contacts (Burt, 1992). In a supply chain, a structural hole exists if two firms share a relationship with a third firm but are not related to each other. This third firm, known as the *tertius*, can gain an advantage by bridging the structural hole, obtaining information and control benefits relative to the two disconnected actors (Burt, 1992). Information benefits can come about in three ways: access (i.e. receiving valuable information not accessible to all actors), timing (i.e. receiving information before other actors) and referrals (i.e. providing more opportunities). Control stems from being the third party that connects and brokers (or chooses not to broker) the other two (Zaheer *et al.*, 2010; Li and Choi, 2009; Burt, 1992).

Burt (2004) shows that structural holes in a network of individuals can provide benefits through the creation of ideas and the acceptance of these ideas by other network members. At an organizational level, Walker *et al.* (1997) reveal that entrepreneurial firms can exploit structural holes in the network. While the benefits of structural holes for creativity, innovation and flexibility have been documented, a parallel stream of research posits that structural holes can expose network members to opportunistic behavior and undermine cooperation among firms, and even lead to unethical and criminal behavior (Brass *et al.*, 1998; Sparrow, 1991). Ahuja (2000) finds that structural holes can also hurt innovation, and Hernandez *et al.* (2015), find that network closure can act as a defensive approach against information leakage. Ultimately, some authors have concluded that structural holes offer network members a bright and a dark side (Gargiulo and Benassi, 2000). Given that this research focuses on fraud, our perspective concentrates on how to identify and avoid the dark side. Burt's emphasis is on the firm taking the position of structural advantage; conversely, in this investigation, we focus on the firms in the disadvantageous position of being structurally exposed to fraud.

It has been theorized that firms bridging a structural hole have two alternative strategic orientations: *tertius gaudens* and *tertius iungens*. The *tertius gaudens*, or third who rejoices, takes advantage of its position, brokering the connection between the other parties (Burt, 1992), taking control and exploiting information asymmetries (Zaheer and Bell, 2005).

Following the *tertius gaudens* approach, a firm could choose to act opportunistically by strategically manipulating the other two parties (Shi *et al.*, 2009); and, as Burt (1992, p. 33) acknowledges, it may choose to exchange "ambiguous, or distorted information" to take advantage. Conversely, the *tertius iungens*, or third who joins, connects the other parties in the network by "either introducing disconnected individuals or facilitating new coordination between connected individuals" (Obstfeld, 2005, p. 102) and is a more benevolent orientation.

A way to prevent the *tertius* from taking advantage of its structural position is to alter the network's structure. This restructuring could happen either if the other two actors in the supply chain establish a connection, undermining the bridge position and eventually making it redundant (Burt, 2002; Li and Choi, 2009; Johnson, 2004); or if the *tertius* decides, willingly or unwillingly, to relinquish its position, transferring the bridge to another firm (Li and Choi, 2009). In both situations, the structure of the network changes, either by closing the structural hole (bridge decay) or by moving the structural hole (bridge transfer), and thus alters the ability of the *tertius* to act opportunistically. Burt (2002) also acknowledges that the bridge position can also decay over time (Burt, 2002), so the unscrupulous actor needs to devote efforts to prevent decay.

Structural holes theory delineates two possible orientations for the *tertius* as either cooperative (*iungens*) and opportunistic (*gaudens*), but it does not consider an orientation where the *tertius* is actively or passively causing harm with malicious intent. Furthermore, structural holes theory does not focus on the roles of the other actors in the triad. Extending the triadic perspective can provide greater insight into the relationship configuration in supply chain networks, particularly when it comes to trust and monitoring behaviors in a network (Meqdadi *et al.*, 2020).

Firms can intentionally adjust the structure of their network to prevent knowledge leakage to competitors (Hernandez *et al.*, 2015). To explain how a firm reshapes its connections, Hernandez *et al.* (2015) propose three deliberate mechanisms: pruning (terminating ties), grafting (avoiding new ties) and closing (seeking densely connected networks). While Hernandez *et al.* (2015) describe the network-level defensive mechanisms, a firm can employ, an unscrupulous firm can use similar network-level mechanisms in an offensive way. Thus, a firm can deliberately alter the structure of the network with the intent of defrauding other parties.

Theoretical elaboration: the constructs of structural supply chain fraud

Evidence from the case studies suggests that understanding the supply chain structure of the fraud is critical to understanding how the fraud emerged. To do so, we propose a new orientation called the *tertius fraudans*, or the third who cheats. For structural supply chain fraud to occur, a minimum of three actors is needed: a perpetrator (*tertius fraudans*), a victim and an enabler. Figure 2 depicts a basic structure of supply chain fraud, compared to that of Mattel which shows an extension of that network structure. In this structure, the *tertius fraudans* acts as a bridge, and uses its position to gain advantage fraudulently. The structure incorporates the three main roles; however, these roles may extend beyond the triad so that multiple victims, multiple enablers and even multiple fraudsters may play a role in, as evidenced in the networks from each case study.

The *tertius fraudans* is the actor who perpetrates the fraud. Like the *tertius gaudens,* the *tertius fraudans* benefits from information asymmetries, but in this case, the *tertius* engages in an unlawful act and has malicious intent. Here, the *tertius fraudans* seeks to create a structure that gives them an advantage in terms of information asymmetries and then exploits this advantage causing harm to the victim(s). Additionally, the *tertius fraudans* can create information asymmetries through deceptive acts of omission or commission. This is most clearly evidenced in the Takata case study. Takata deleted test data to hide problems from downstream actors to further their own self-interest. Similarly, though to a less egregious degree, Honda selectively hid information from their customers.

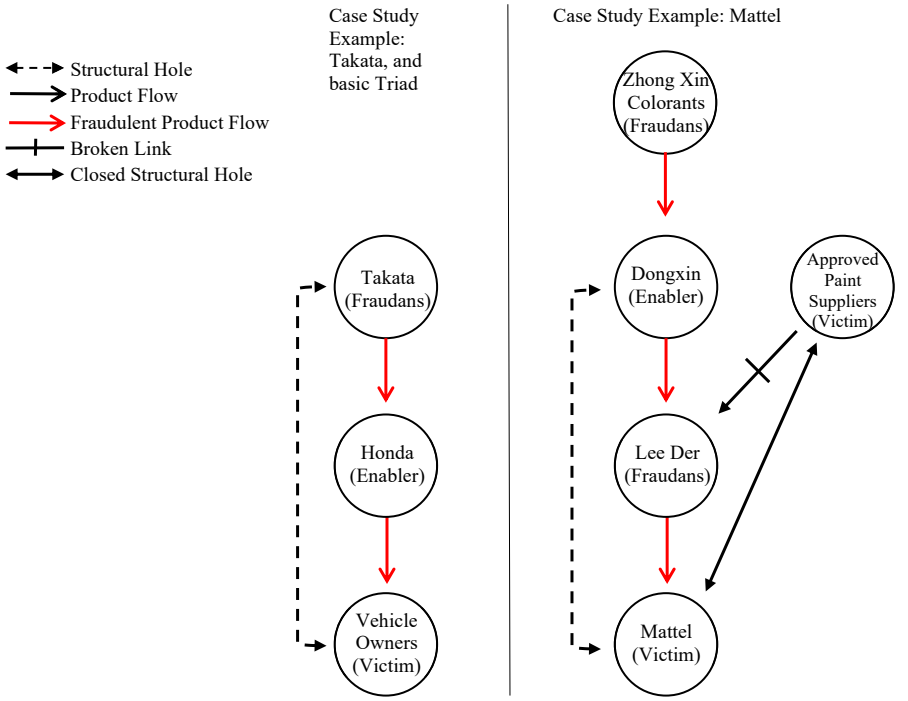


Figure 2.
Basic fraudans structure with structural hole and Mattel example

The example on the left demonstrates the simplest structure for supply chain fraud, though the order of fraudans/enabler/victim could be changed in other examples. The example on the right is from the Mattel case study, showing the role of structural holes. These two examples from the case studies illustrate the role of structural holes in enabling a *tertius fraudans*

An unscrupulous firm might also manipulate the network structure to position itself in the bridge position. In both the Mattel case and the horsemeat case, suppliers circumvented approved supplier lists to source from unapproved suppliers, positioning themselves as a bridge over a structural hole, rather than a network with a closed structure. This manipulation of the network, undetected by Mattel and Tesco, was what enabled fraudulent product to enter the supply chain.

In a *tertius fraudans* structure, the enabler is the actor who provides the means through which fraud can occur and provides support to the *tertius fraudans*. This can be by knowingly supplying products to a buyer who then sells the products fraudulently by making false claims about them. Or it could be a firm aware that a supplier that is acting fraudulently and providing a platform through which those products can be distributed. Finally, the victim is the actor who suffers the consequences of fraud and can include individual consumers or companies that are defrauded.

Table 4 combines the original roles described in structural holes theory with the new roles proposed for structural supply chain fraud, summarizing the main characteristics of each role. We next discuss these main characteristic as it relates the structural fraud.

Theoretical foundation: structural holes and the tertius fraudans

While Burt (2002) acknowledges that a *tertius* can sometimes exchange ambiguous or distorted information to take advantage, he does not refer to fraudulent activity, and in fact

	Structural holes theory		Structural supply chain fraud		
Terminology	*Tertius Iungens*	*Tertius Gaudens*	*Tertius Fraudans*	*Victim*	*Enabler*
Meaning	"The Joining third"	"The rejoicing third"	"The cheating third"		
Behavior	Cooperative	Opportunistic	Unlawful and deceptive	Suffers harm	Provides means or opportunity
Orientation /Role	Benevolent	Self-interested	Malicious	Unaware	Enabler
Outcome for main actor	Positive	Mixed[1]	Positive (but with risks)	Negative	Positive or Neutral
Bridging Mechanics	Bridge transfer	Bridge decay	Bridge decay and bridge collapse		

Note(s): [1]Provides advantages, but also increases risks

Table 4. Combining structural holes theory to include supply chain fraud

emphasizes the social capital benefits of the bridge position and encourages firms (and individuals) to create bridges and seek a *tertius* position. Given the position of fraud as an extreme form of opportunism, the conditions of a structural hole also provide the means for a *tertius fraudans* to engage in fraudulent actions.

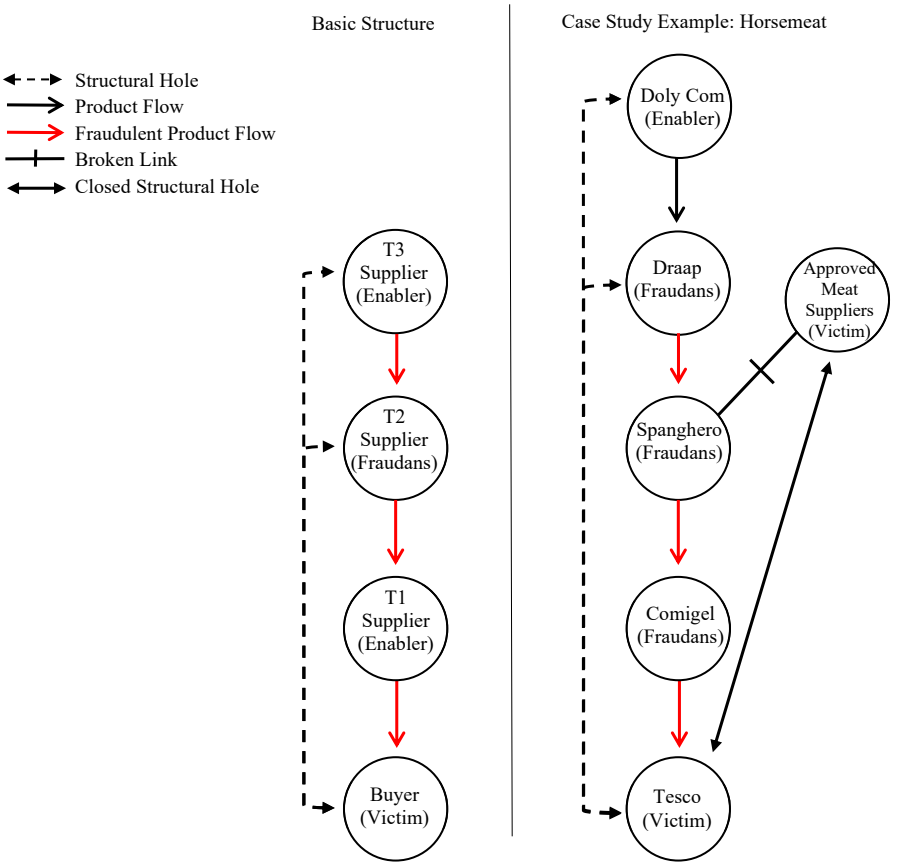
Unscrupulous firms enable fraud by changing network structures to create or transfer a bridge that positions them as the *tertius fraudans*. Indeed, it is likely that once the fraudulent product enters the supply chain through an unauthorized network source, the fraud is passed through multiple tiers of firms who believe they are purchasing a legitimate product, since the main goal of a fraudster is to leverage information asymmetries. To alleviate concerns regarding structural holes, researchers have proposed that bridging structural holes, through bridge decay, can help to reduce opportunistic behavior (Li and Choi, 2009).

Theoretical elaboration: structural holes and the tertius fraudans

The case studies reveal how structural holes serve as a mechanism for structural supply chain fraud to occur. For instance, Takata utilized the structural hole between the automotive assemblers and the suppliers of raw materials to adopt a *tertius fraudans* position where they were able to use their informational advantage to hide product risks. Takata switched to a cheaper but less stable explosive propellant for its airbag inflators and hid knowledge of the product risks from the automotive manufacturers by deleting test-data (Trudell and Fisk, 2016). This position allowed them to buy the inferior material and then fraudulently deceive the original equipment manufacturer (OEMs) regarding the risks.

In Takata's case, a series of incidents, injuries and deaths over ten years, lead to an investigation of the role of airbags in these accidents. During the investigation, the structural hole was bridged as information from the suppliers, including Takata, came to light, revealing the depth of their fraud. This investigation resulted in the largest automotive recall in history (Ivory and Tabuchi, 2015) and the eventual bankruptcy of Takata (Soble, 2017). This situation led to a sudden collapse of the supply network structure as firms rushed to replace the supplier while trying to source sufficient airbags. While in the case of Takata, a formal investigation was necessary to close the structural hole, it is also possible for firms to accelerate bridge decay by simply connecting with previously unconnected network actors.

A case involving victims, perpetrators and enablers at multiple supply chain tiers is the horse meat scandal that plagued Europe in 2013. The *tertius fraudans* here were two meat processing companies Spanghero and Silvercrest Foods, who appear to have deliberately adulterated beef with cheaper horse meat (Brooks *et al.*, 2017; European Commission, 2014). In the case of Spanghero, depicted in Figure 3, horse meat was supplied by a Romanian company



This is an example illustrating how enablers can facilitate a fraudans actor at multiple parts in the supply chain. In this case, a tertius fraudans (T2 Supplier) is able to source fraudulent product from an enabler (T3 Supplier) without the buyer's knowledge. The product is sold to another enabler, (T1 Supplier), which serves as an additional layer of obfuscation that further hides the fraudulent behavior. This network structure is a simplified version of the fraud that led to horsemeat scandal (depicted on the right)

Figure 3.
Fraudans structure with enablers and horsemeat case example

that labeled the meat as horse, and then claimed to be an ignorant bystander unknowingly enabling fraud (BBC News, 2013). However, the supplier of horsemeat was led by a previously convicted fraudster known for selling horsemeat as beef and named his company "Draap"–which is "horse" in Dutch spelled backward. Another enabler of fraud in this case was Comigel, who sold products containing horsemeat, in some cases 100% horsemeat, to grocers for up to six months (Falkheimer and Heide, 2015; Hickman, 2013). Caterers like the Compass Group and retailers like Tesco and Aldi appear to be victims, as they were unknowingly supplying adulterated products. When they became aware of the fraud, they withdrew these products, introduced additional controls and severed relationships with the fraudulent suppliers (Yamoah and Yawson, 2014). This fraud was possible because the victims were disconnected from the suppliers of raw materials (horsemeat) through a convoluted supply chain structure

that included both a digital ordering process and a physical transfer of products that created structural holes to hide the original source of products (BBC News, 2013).

Evidence from all five cases was largely consistent regarding the role of the of the *tertius fraudans* abusing a bridge position, suggesting that structural holes serve as an important condition for structural supply chain fraud to occur. Of the five cases analyzed, four of them (Mattel, Horsemeat, Fitbit, and Maui Jim) demonstrate clear structural holes, and the fifth (Takata) demonstrates a structural hole that is less obvious, but consists of informational advantages between the tiers as each company serves as a bridge. Many of the networks demonstrated multiple structural holes that were leveraged by the *tertius fraudans* to take advantage of information asymmetries and engage in fraud.

In two of the cases, when these structural holes were closed (Mattel, Horsemeat), the *tertius fraudans* created a new link to bypass the closed structural hole, creating a network with structural holes that enabled them to circumvent the structural controls implemented by the victims. In the cases of Fitbit and Maui Jim, there was originally no obvious structural hole, since the network seemed complete; however, the *tertius fraudans* created new links and structural holes that obfuscated the fraud both upstream and downstream.

In the cases of Mattel, and Horsemeat scandal, the fraud unraveled when it was discovered by external groups who identified the fraud and the structural holes. However, investigating the fraud required closing structural holes to identify the depth of malfeasance, at which point both groups created new protection mechanisms to prevent future fraud. In the case of Fitbit, a case of potential counterfeit products in the market led to discovery of the fraudulent network structure and ultimately resulted in the closure of the structural hole. In the Takata case, the fraud was not fully revealed until external groups investigated the situation and addressed the information asymmetry by acquiring internal evidence from the responsible parties. Finally, the Maui Jim case demonstrated a resistance to closing the structural hole, and much of the legal battle focused on how much of the unauthorized supply chain would need to be disclosed. Overall, this supports that closing the structural hole can reveal the *tertius fraudans* and help prevent future fraud.

We argue that closing structural holes can help prevent fraud by making supply chains more transparent and eliminating information asymmetries, preventing parties from adopting a *tertius fraudans* position and revealing the existence of *tertius fraudans* if detected.

Proposition 1a. Structural holes in a network allow supply chain actors to adopt a *tertius fraudans* role.

Proposition 1b. Firms acting *as tertius fraudans* alter the structure of their networks to enable fraud.

Proposition 1c. Closing structural holes through bridge decay can reveal the *tertius fraudans* and prevent future fraud.

Theoretical foundation: structural ignorance and fraud

While eliminating structural holes might be possible when firms are operating in good-faith such as *tertius iungens*, it is more difficult to convince a firm who takes advantage of their *tertius fraudans* position to relinquish informational control. In addition, even in the absence of structural holes, firms can engage in fraudulent actions enabled by their network structure. This is a particular challenge when firms are willing to circumvent the norms controlling the relationship and engage in deceptive behavior. An example of such behavior would be the case of supplier collusion where suppliers colluding to artificially inflate the prices (Simangunsong *et al.*, 2016).

We propose extending the structural holes theory by introducing a new network construct that needs to be considered as a potential enabler and preventer of structural supply chain fraud. We call this structural ignorance, which we define as a firm's lack of awareness of a linkage that one of its connected firms has with another firm in the supply chain. Structural ignorance plays a role in different kinds of fraudulent behavior in addition to supplier collusion. Fraud can be enabled by a firm creating a new underlying network structure without the victim in the supply chain being aware of it. Indeed, it is likely that once a fraudulent product enters the supply chain through an unauthorized network source, the fraud is passed through multiple tiers in the supply chain who believe they are purchasing a legitimate product. For example, counterfeit manufacturing can occur as suppliers make additional runs of products (midnight runs) and sell the unauthorized components to other buyers or to a black-market distributor.

Structural ignorance serves as an additional mechanism through which information asymmetries can be abused. In this case, the fraudulent firm benefits, not by creating or transferring a bridge position, but by disguising the structure and composition of the network. If a victim firm is unaware of the nature of relationships between other parties in the network, fraudulent firms can use leverage knowledge asymmetries for fraudulent behaviors. The actors who bridge structural holes to their advantage may seek to recreate such holes, and thereby wish the, to remain hidden (Zaheer and Soda, 2009). *Tertius fraudans* firms can further rely on this by intentionally manipulating other members' knowledge of the structure of the network, by hiding ties or by implying the existence of non-existent ties.

The key theoretical driver of this relationship is still information asymmetry within the network (Zaheer and Soda, 2009). However, the information that is missing is information regarding the structural connections within the network. Firms that identify the structural connections within their supply chain network, i.e. have network transparency about linkages, can be better positioned to limit structural supply chain fraud and prevent additional cases of this type of fraud from occurring.

To alleviate fraud resulting from structural ignorance, firms that can track flow of products within their entire supply chain can reduce the structural ignorance associated with product-fraud. These efforts are effective, though imperfect, mechanisms that firms can use to mitigate the risks associated with fraud. Supply chain tracking and transparency is particularly important for types of fraud with high likelihood of occurrence and where buyers face severe consequences (Shevchenko *et al.*, 2020).

Theoretical elaboration: structural ignorance and fraud

The cases studies showed that *tertius fraudans* will intentionally manipulate the information available so that the true nature of the relationships in the supply chain and the provenance of the materials are unknown in order to leverage the information asymmetry to perpetrate the fraud. For example, in the Fitbit case, a complex network of firms was created obfuscating the fraud from both upstream and downstream in the supply chain. As depicted in Figure 4, the primary structural mechanism is not a structural hole in the relationship, but rather the ignorance of the structural connection that the supplier has with an alternative and unauthorized supply chain.

Fitbit learned that unauthorized and faulty products were being sold by Groupon, but was completely unaware of how those products were entering the supply chain and had to ask Groupon to identify their supplier. The products were being supplied from within Fitbit's own reverse supply chain, but because Fitbit was unaware of the recycler's links, it did not know that it was the source of faulty products.

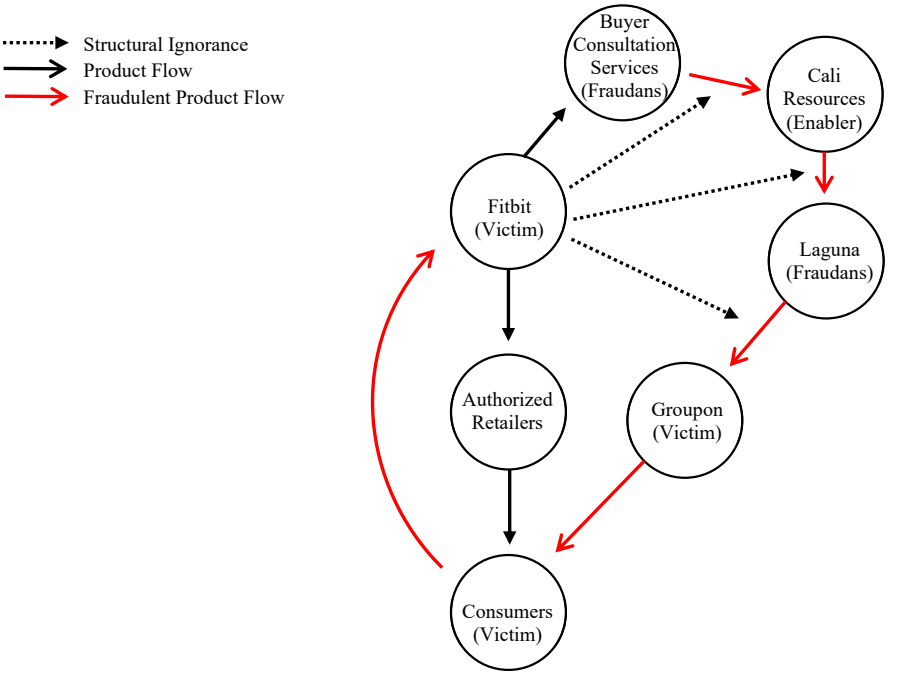


Figure 4.
Fitbit cast study example of fraud obfuscation through structural ignorance

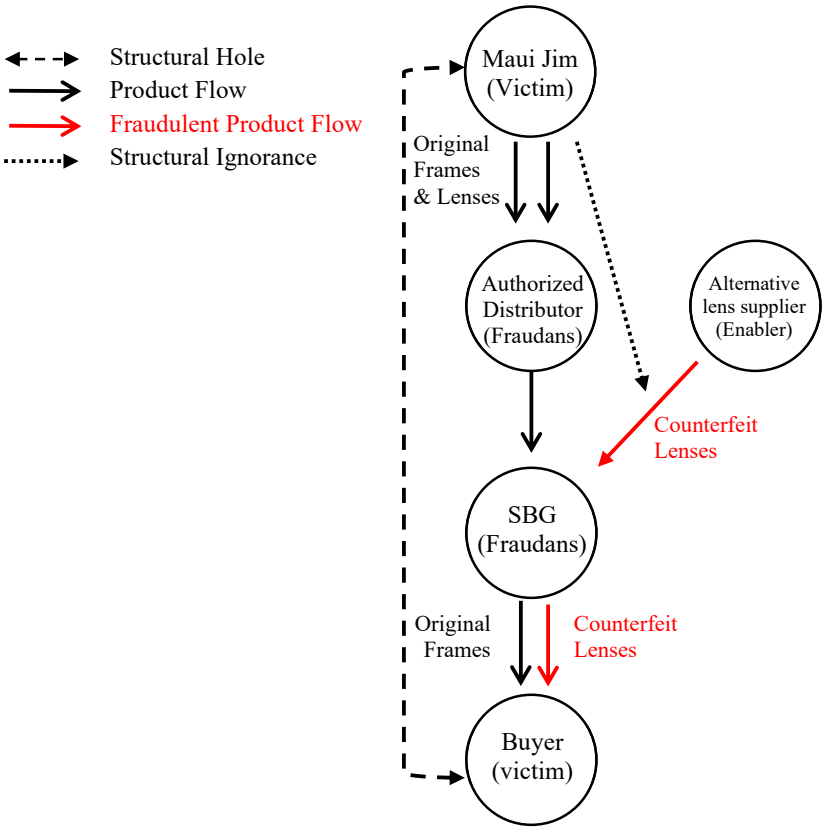
This is an example illustrating the complicated network structure that can be created, obfuscating the source of the fraud from both Groupon and Fitbit. The network structure was unknown until Fitbit connected with Groupon, and began closing the structural holes to identify that scrap product was reentering the supply chain via their recycler

In the Maui Jim case, an authorized distributor created a secondary fraudulent supply chain. This positioned the company as a double bridge, enabling opportunistic behavior from its novel supply chain structure that Maui Jim was unaware of. Despite Maui Jim being fully aware of the authorized network, if a firm is simply unaware that the other network actors have a covert connection or is unaware of the unethical nature of relationships among other actors, these unscrupulous actors can exploit the structure to collude, as can be seen in Figure 5.

In the Takata case study, Honda was aware of the supply chain network, but information asymmetries were used to enable fraud. The evidence suggests that the role of a firm occupying a bridge position enables fraud by providing them the means to control the information that passes the bridge (Zaheer and Soda, 2009), allowing them to conduct fraudulent behavior.

The role of structural ignorance was largely consistent across the other case studies. In four cases (Mattel, Horsemeat, Fitbit, Maui Jim), structural ignorance played a key role to create information asymmetries that were exploited. In these cases, the victim firms were unaware of the network structure and the relationships between the fraudulent companies that enabled fraud to occur. In the Fitbit case, multiple parties chose not to disclose their supply chain in court and in communications, perhaps in order to recreate these structural holes elsewhere (Zaheer and Soda, 2009).

In these four cases, the *fraudans* intentionally created structural ignorance to disguise the composition of the network to enable fraud. The networks were hidden from the



This example illustrates a double bridge (a structural hole spanning across two firms) between a buyer and Maui Jim, the original equipment manufacturer of frames and lenses. Both the authorized distributor and SBG are acting opportunistically to defraud Maui Jim and the customer, by reselling goods without authorization and introducing counterfeit lenses into the supply chain

Figure 5.
Maui Jim's case study example of secondary fraudulent supply chain

victims and then further exploited. In three of the cases (Horsemeat, Fitbit, Maui Jim) after discovery of potential fraud, firms were reluctant to reveal the network structure. Overall, the evidence supports the notion that *tertius fraudans* firms create structural ignorance to disguise fraud and eliminating structural ignorance through transparency can reveal fraud.

Proposition 2a. Structural ignorance in a network creates information asymmetry and enables *tertius fraudans* behavior to occur through the unknown structural relationship.

Proposition 2b. *Tertius fraudans* firms intentionally create structural ignorance to disguise the structure and composition of the network and enable fraud.

Proposition 2c. Reducing structural ignorance in a network through transparency can reveal the *tertius fraudans* and prevent future fraud.

Theoretical foundation: the role of bridges in structural supply chain fraud

Structural holes theory acknowledges that the dynamics of a triad or network can change over time, and so a bridge can be transferred from one firm to another (Li and Choi, 2009) or the bridge position can simply decay over time (Burt, 2002). When fraudulent behaviors in a supply chain are unveiled, it is likely that bridges will adapt. Two possible outcomes can be foreseen when a firm unveils a fraud–either it accepts the fraudulent behavior, for example, passing the fraudulent product on to their customers without addressing the issue, becoming an accomplice (enabler) to the fraud, or it seeks to eradicate the fraud. For the majority of cases, firms seek to remove the bridge (i.e. close the hole) and reduce structural ignorance to limit fraud to prevent fraud from reoccurring.

While slow bridge decay might be sufficient for preventing opportunistic or fraudulent behaviors from occurring in the future, once a fraud is discovered, the recovery process must commence rapidly. We call the events following the discovery of a *tertius fraudans* bridge collapse, as it triggers a cascade effect that swiftly undermines a bridge position, hindering the possibility for continuation of the fraud and requires rapid changes to the supply chain.

Theoretical elaboration: role of bridges in structural supply chain fraud

When the evidence of fraud is uncovered, the reaction from the affected parties is often immediate and significant. In several of the cases, there is strong evidence that immediate and conclusive actions were taken to protect the integrity of the supply chain. For example, in the Horsemeat scandal, suppliers accused of providing horsemeat were immediately dropped. This is particularly notable as when Irish Burger King found out it had bought meat from an involved supplier changed suppliers prior to completing tests to verify if they had been affected (Falkheimer and Heide, 2015). In the Fitbit case, the company severed relationships with the firms selling their scrapped products, as soon as the fraud became evident. Similarly, in the Maui Jim case, the company quickly severed relationships with the authorized distributor, and sued SBG, the unauthorized distributor.

Which thus posits that uncovering the evidence of fraud will lead to bridge collapse as clearly supported in three cases (Horsemeat, Fitbit, Maui Jim). One case (Takata) suggested partial bridge collapse. Due to lack of immediate industry capacity, Takata remained in the relationship and produced many of the replacement airbags for the recall, though over time they were replaced in network structure and ultimately declared bankruptcy. As an exception, it appears that Mattel maintained the relationship with their supplier rather than cut ties. This suggests that while bridge collapse is a potential remedy after discovering fraud, though other mechanisms that rely on social or contractual governance also serve as potential remedies.

Proposition 3. Uncovering the intentions and/or actions of a *tertius fraudans* will bring about bridge collapse, requiring a swift restructuring of the network.

Divergent themes

Convergent themes across the case studies and the theoretical foundations allowed us to formulate a series of propositions. However, the cases also revealed some divergent themes for which we do not have sufficient evidence to formulate propositions, but appear worthy of further investigation. In particular, two divergences are worth noting: the complexity of the networks and the motives behind the fraud.

The complexity of the networks ranged from simple, as in Takata, depicted in Figure 1, to highly complicated network structures, as in Fitbit, depicted in Figure 4. In general, the network structures where fraud was perpetuated tended to evolve into highly complex networks which could be used to obfuscate the fraud, though this is not necessarily the case in

all fraud examples and so should be considered a sufficient, but not necessary, antecedent condition for fraud to occur.

While the prospect of economic gains is consistent across all cases, additional motives behind the fraud also exhibited substantial variation. One case seems to be driven primarily by profits (Horsemeat). Two cases (Fitbit and Maui Jim) seem to be driven primarily by access to products that were only obtained through potentially dubious means but that enabled significant profit advantages. Two other cases seemed to be driven by significant pressures (in the case of Mattel: time pressure and product availability; and in the case of Takata, company viability and cost-reduction pressures to survive). If considered from one of the prominent theories on fraud, the Fraud Triangle (see Cressey, 1953; DuHadway *et al.*, 2020; Arnold *et al.*, 2012), the motives primarily seemed to center around opportunity and pressure. Given significant pressures, firms found ways to survive, even if those ways included deceptive self-interest seeking, and given significant opportunity to engage in fraud, including a lack of adequate oversight and controls, firms found ways to take advantage of that situation for profit.

Contributions and conclusions

Theoretical implications

In this paper, emphasize the importance of a structural perspective on fraud. We do this by elaboration on structural holes theory in the context of structural supply chain fraud. First, we develop the construct of structural supply chain fraud, which can be used by other scholars and provides a starting point for a conversation about this phenomenon.

Second, in the first set of propositions, we introduce the concept of *tertius fraudans* into social network theory. In proposition 1a, b and c, we show how structural holes and structural ignorance can enable fraud and that by eliminating them, firms are able to identify structural fraud, *tertius fraudans* and prevent future fraud. We provide a framework for understanding the roles of various supply network actors in structural supply chain fraud and examples that demonstrate the relevance of the network perspective on discussing and understanding structural supply chain fraud.

Third, we introduce the concept of structural ignorance, which refers to a firm's lack of awareness of a linkage between one of its connected firms and another firm in the supply chain. In propositions 2a and b, we illustrate that what you do not know can hurt you when a fraudulent actor takes advantage of its knowledge of network structure to commit fraud. We show how structural ignorance can lead to fraud, and provide examples of how structural ignorance can be reduced or eliminated, diminishing the opportunity for structural supply chain fraud. These findings are also very relevant to managers in their efforts to prevent this kind of fraud, as indicated in proposition 2c and expanded below.

Fourth, we introduce the concept of bridge collapse in proposition 3 and demonstrate how organizations can defend themselves against fraud and the structural outcomes once fraud is discovered. This has both theoretical and practical implications as it not only helps to explain the phenomenon, but also proposes that through a deliberate process of bridge collapse rather than a gradual bridge decay, firms can quickly undermine the position of the *tertius fraudans* and thus prevent and recover from fraud. Following a bridge collapse, firms need to rapidly engage in bridge reconstruction to restructure the supply network, either by eliminating structural holes or structural ignorance, and by replacing the *tertius fraudans*.

Managerial implications

To be useful, theory should have practical implications (Van de Ven, 1989). Structural supply chain fraud is a large and important problem that can cause significant supply chain

disruption and hurt companies financially and reputationally. By casting structural supply chain fraud from a network perspective, we help managers understand how fraud can occur in their supply networks and provide insight into where in a supply network such fraud might occur. We also provide suggestions regarding how to prevent structural supply chain fraud through supply chain structural decisions, and how to recover quickly should fraud occur. Finally, we reinforce the idea that what you do not know about your supply chain can hurt you. In this case, ignorance is not bliss, and supply chain transparency is desirable.

Fraud is a common problem that affects supply chain performance, not only because it has negative financial consequences, but also because it can have operational and reputational implications for all firms involved. Fraud across supply chains is a prevalent concern in industry, yet there is little scientific discussion of the problem. We seek to provide a greater scientific understanding of fraud to provide managers with meaningful tools to combat the global challenge of fraud.

We identify three key mechanisms for managers to emphasize to reduce structural supply chain fraud. First, by reducing the number of structural holes in a critical supply chain structure, network, and thus negating high risk opportunities for a potential *tertius fraudans*. While it is likely not possible to close every structural hole in a network, firms can establish stronger linkages across tiers for critical parts of the supply chain. For example, if a focal firm requires a supplier to buy from approved suppliers by placing an order through the focal firm to the approved supplier, it would be difficult to circumvent the fully closed structural hole. Second, by gaining a better understanding of the overall network structures and linkages, managers reduce the information asymmetry that creates the potential for fraud, and increase supply chain transparency. Third, by consciously building relationships with second tier suppliers of critical inputs, managers can reduce the likelihood of receiving goods produced with fraudulent materials, varying the degree of control over the first and second tier supplier relationship based on the likelihood of fraud and the magnitude of its impact. As transparency is increased, managers will be able to identify fraud and prevent future fraud from occurring.

Limitations and further research. Fraud is a challenging topic for empirical research because it tends to be a covert activity, making it difficult to find reliable sources of information. One limitation of this research is that it is based entirely on secondary data, based on what those close to the fraud were willing to reveal publicly or as part of a lawsuit, or as the press inferred. It is not clear whether important information is lacking, as victims are often embarrassed and do not want to reveal everything, and fraudsters do not want to reveal the tricks of their trade and their networks, so that they can potentially be revisited in the future. In addition, we have focused on the under-researched area of structural fraud. There is a robust stream of research that investigates the role of contracts and relationships in facilitating or preventing fraud. Future research should combine these perspectives with supply chain structural fraud to get a more complete view of how these mechanisms can most effectively work together to reduce, detect and prevent supply chain fraud.

Structural fraud in the supply chain is an important topic with strong potential for theory building and practical relevance, worthy of further investigation. For example, how do issues such as trust, discovery, disclosure, uncertainty and risk moderate structural fraud in the supply chain? We explored the issue of fraud motivation, but our results did not converge. This is also a worthy topic of study, and could provide insight into prevention and detection of structural supply chain fraud. We intend to continue this investigation using behavioral experiments, where we can put participants in hypothetical situations where they are likely to feel more comfortable expressing their views. An alternative avenue for research would be to use secondary evidence from documented cases of fraud to investigate how the structural characteristics of supply networks affect fraud. Using these approaches, we intend to test and further develop the propositions presented in this paper.

References

Ahuja, G. (2000), "Collaboration networks, structural holes, and innovation: a longitudinal study", *Administrative Science Quarterly*, Vol. 45 No. 3, pp. 425-455.

Arnold, U., Neubauer, J. and Schoenherr, T. (2012), "Explicating factors for companies' inclination towards corruption in Operations and supply chain management: an exploratory study in Germany", *International Journal of Production Economics*, Vol. 138 No. 1, pp. 136-147.

Association of Certified Fraud Examiners (2016), *Report to the Nations on Occupational Fraud and Abuse. 2016 Global Fraud Study*, Association of Certified Fraud Examiners Austin, TX.

BBC News (Producer) (2013), "Q&A: horsemeat scandal", April 27, 2019, available at: https://www.bbc.com/news/uk-21335872.

Brass, D.J., Butterfield, K.D. and Skaggs, B.C. (1998), "Relationships and unethical behavior: a social network perspective", *Academy of Management Review*, Vol. 23 No. 1, pp. 14-31.

Brooks, S., Elliott, C.T., Spence, M., Walsh, C. and Dean, M. (2017), "Four years post-horsegate: an update of measures and actions put in place following the horsemeat incident of 2013", *Npj Science of Food*, Vol. 1 No. 1, p. 5.

Burt, R.S. (1992), *Structural Holes: The Structure of Social Capital Competition*, Harvard University Press, MA Cambridge.

Burt, R.S. (2002), "Bridge decay", *Social Networks*, Vol. 24 No. 4, pp. 333-363.

Burt, R.S. (2004), "Structural holes and good ideas", *American Journal of Sociology*, Vol. 110 No. 2, pp. 349-399.

Center for Disease Control and Prevention (2021), "Counterfeit respirators/misrepresentation of NIOSH – approval", available at: https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html (accessed 10 November 2021).

Child, J. and Rodrigues, S.B. (2003), "Corporate governance and new organizational forms: issues of double and multiple agency", *Journal of Management and Governance*, Vol. 7 No. 4, pp. 337-360.

Choi, T.Y. and Wu, Z. (2009), "Taking the leap from dyads to triads: Buyer–supplier relationships in supply networks", *Journal of Purchasing and Supply Management*, Vol. 15 No. 4, pp. 263-266.

Coase, R.H. (1937), "The nature of the firm", *Economica*, Vol. 4, p. 386.

Cressey, D.R. (1953), *Other People's Money: A Study in the Social Psychology of Embezzlement*, Free Press.

DiMaggio, P.J. and Powell, W.W. (1983), "The iron cage revisited: institutional isomorphism and collective rationality in organizational fields", *American Sociological Review*, Vol. 48 No. 2, pp. 147-160.

DuHadway, S., Carnovale, S. and Hazen, B. (2019), "Understanding risk management for intentional supply chain disruptions: risk detection, risk mitigation, and risk recovery", *Annals of Operations Research*, Vol. 283 No. 1, pp. 179-198.

DuHadway, S., Talluri, S., Ho, W. and Buckoff, T. (2020), "Light in dark places: the hidden world of supply chain fraud", in *IEEE Transactions on Engineering Management*, doi: 10.1109/TEM.2019.2957439, available at: https://ieeexplore.ieee.org/abstract/document/8948004.

Eisenhardt, K.M. (1985), "Control: organizational and economic approaches", *Management Science*, Vol. 31 No. 2, p. 134.

Eisenhardt, K.M. (1989), "Agency theory: an assessment and review", *Academy of Management Review*, Vol. 14 No. 1, pp. 57-74.

European Commission (2014), "Horse meat (2013-14)", available at: https://ec.europa.eu/food/safety/official_controls/eu-co-ordinated-control-plans/horse_meat_en (accessed 29 July 2019).

Falkheimer, J. and Heide, M. (2015), "Trust and brand recovery campaigns in crisis: findus Nordic and the horsemeat scandal", *International Journal of Strategic Communication*, Vol. 9 No. 2, pp. 134-147.

Firozabadi, B.S., Tan, Y.-H. and Lee, R.M. (1998), "Formal definitions of fraud", in McNamara, P. and Prakken, H. (Eds), *Norms, Logics and Information Systems – New Studies in Deontic Logic and Computer Science*, IOS Press, pp. 275-288, available at: https://www.google.com/books/edition/Norms_Logics_and_Information_Systems/Efz2tm2BwkIC?hl=en&gbpv=0.

Freeman, L.C. (1979), "Centrality in social networks: conceptual clarification", *Social Networks*, Vol. 1, pp. 215-239.

Freeman, L.C., White, D.R. and Romney, A.K. (1992), *Research Methods in Social Network Analysis*, Transaction Publishers, New Brunswick, NJ.

Fulmer, A.C. and Gelfand, M.J. (2012), "At what level (and in whom) we trust: trust across multiple organisational levels", *Journal of Management*, Vol. 38 No. 4, pp. 1167-1230.

Gargiulo, M. and Benassi, M. (2000), "Trapped in your own net? Network cohesion, structural holes, and the adaptation of social capital", *Organization Science*, Vol. 11 No. 2, pp. 183-196.

Hempel, C.G. (1970), "On the 'standard conception' of scientific theories", in Radner, M. and Winokur, S. (Eds), *Minnesota Studies in the Philosophy of Science*, University of Minnesota Press, Minneapolis, Vol. 4, available at: https://conservancy.umn.edu/handle/11299/184647.

Hernandez, E., Sanders, G. and Tuschke, A. (2015), "Network defense: pruning, grafting, and closing to prevent leakage of strategic knowledge to rivals", *Academy of Management Journal*, Vol. 58 No. 4, pp. 1233-1260.

Hickman, M. (2013), "Horsemeat scandal: findus leak reveals horse in 'beef' for six months, the Independent", available at: https://www.independent.co.uk/news/uk/home-news/horsemeat-scandal-findus-leak-reveals-horse-in-beef-for-six-months-8486602.html (accessed 20 July 2019).

Interpol (2020), "Global operation sees a rise in fake medical products related to COVID-19", [Press release], available at: https://www.interpol.int/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19.

Ivory, D. and Tabuchi, H. (2015), "Airbag recall widens to 34 million cars as Takata admits defects", *The New York Times*, May 20, 2015, p. A1.

Jensen, M.C. and Meckling, W.H. (1976), "Theory of the firm: managerial behavior, agency costs and ownership structure", *Journal of Financial Economics*, Vol. 3 No. 4, pp. 305-360.

Johnson, J.D. (2004), "The emergence, maintenance, and dissolution of structural hole brokerage within consortia", *Communication Theory*, Vol. 14 No. 3, pp. 212-236.

Jones, C., Hesterly, W.S. and Borgatti, S.P. (1997), "A general theory of network governance: exchange conditions and social mechanisms", *Academy of Management Review*, Vol. 22 No. 4, pp. 911-945.

Kavilanz, P.B. (2009), "Mattel fined $2.3 million over lead in toys", *CNN Money*, available at: https://money.cnn.com/2009/06/05/news/companies/cpsc/.

Ketokivi, M. and Choi, T. (2014), "Renaissance of case research as a scientific method", *Journal of Operations Management*, Vol. 32 No. 5, pp. 232-240.

KPMG (2010), "India fraud survey report 2010 [Online]", *KPMG*, (accessed 2019).

KPMG (2017), "Supply chain fraud", *KPMG*, available at: https://assets.kpmg/content/dam/kpmg/be/pdf/Markets/supply-chain-fraud.pdf (accessed 2019).

Lawrence, F. (2013), "Horsemeat scandal: the essential guide", *The Guardian*, available at: https://www.theguardian.com/uk/2013/feb/15/horsemeat-scandal-the-essential-guide (accessed 15 Feb 2013).

Lee, Y. and Cavusgil, S.T. (2006), "Enhancing alliance performance: the effects of contractual-based versus relational-based governance", *Journal of Business Research*, Vol. 59, pp. 896-905.

Li, M. and Choi, T.Y. (2009), "Triads in services outsourcing: bridge, bridge decay and bridge transfer", *Journal of Supply Chain Management*, Vol. 45 No. 3, pp. 27-39.

Lumineau, F. and Oliveira, N. (2020), "Reinvigorating the study of opportunism in supply chain management", *Journal of Supply Chain Management*, Vol. 56 No. 1, pp. 73-87.

Macneil, I.R. (1978), "Contracts: adjustment of long-term economic relations under classical, neoclassical, and relational contracts", *Northwestern Law Review*, Vol. 72 No. 6, pp. 854-901.

Miles, M.B. and Huberman, A.M. (1994), *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd ed., Sage Publications, California.

Ngai, E.W., Hu, Y., Wong, Y.H., Chen, Y. and Sun, X. (2011), "The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature", *Decision Support Systems*, Vol. 50 No. 3, pp. 559-569.

Obstfeld, D. (2005), "Social networks, the *tertius iungens* orientation, and involvement in innovation", *Administrative Science Quarterly*, Vol. 50 No. 1, pp. 100-130.

Oliver, C. (1991), "Strategic responses to institutional processes", *Academy of Management Review*, Vol. 16 No. 191, pp. 145-179.

Oxford English Dictionary, *Fraud, n*, Oxford University Press.

Pilbeam, C., Alvarez, G. and Wilson, H. (2012), "The governance of supply networks: a systematic literature review", *Supply Chain Management*, Vol. 17 No. 4, pp. 358-376.

Poppo, L. and Zenger, T. (2002), "Do formal contracts and relational governance function as substitutes or complements?", *Strategic Management Journal*, Vol. 23 No. 8, pp. 707-725.

Rose-Ackerman, S. and Palifka, B.J. (2016), *Corruption and Government: Causes, Consequences, and Reform*, Cambridge University Press.

Selznick, P. (1948), "Foundations of the theory of organizations", *American Sociological Review*, Vol. 13, pp. 25-35.

Sharma, A. (1997), "Professional as agent: knowledge asymmetry in agency exchange", *Academy of Management Review*, Vol. 22 No. 3, pp. 758-798.

Shevchenko, A., Pagell, M., Lévesque, M. and Johnston, D. (2020), "Preventing supplier non-conformance: extending the agency theory perspective", *International Journal of Operations & Production Management*, Vol. 40 No. 3, pp. 315-340.

Shi, W., Markoczy, L. and Dess, G.G. (2009), "The role of middle management in the strategy process: group affiliation, structural holes, and *tertius iungens*", *Journal of Management*, Vol. 35 No. 6, pp. 1453-1480.

Silvestre, B.S., Viana, F.L.E. and de Sousa Monteiro, M. (2020), "Supply chain corruption practices circumventing sustainability standards: wolves in sheep's clothing", *International Journal of Operations & Production Management*, Vol. 40 No. 12, pp. 1873-1907.

Simangunsong, E., Hendry, L.C. and Stevenson, M. (2016), "Managing supply chain uncertainty with emerging ethical issues", *International Journal of Operations and Production Management*, Vol. 36 No. 10, pp. 1272-1307.

Simmons, M.R. (1995), "Recognizing the elements of fraud", available at: https://www.cocfe.org/what-is-fraud.html.

Smith, R.G. (2001), "Defining, measuring, and reporting fraud risk within your organisation", *paper presented at the IIR Conferences, Applying Risk Management to Implement a Proactive Fraud Prevention Strategy in Financial Services*, Parkroyal Darling Harbour.

Soble, J. (2017), "Effects of Takata Bankruptcy to extend far and wide", The New York Times, available at: https://www.nytimes.com/2017/06/26/business/takata-japan-bankruptcy.html (accessed 28 February 2019).

Sparrow, M.K. (1991), "The application of network analysis to criminal intelligence: an assessment of the prospects", *Social Networks*, Vol. 13 No. 3, pp. 251-274.

Stephen, J.F. (1883), *A History of the Criminal Law of England*, Macmillan, Vol. 3.

Trudell, C. and Fisk, M.C. (2016), "Honda audit finds Takata engineers manipulated air-bag test data", *Bloomberg*, available at: https://www.bloomberg.com/news/articles/2016-07-18/honda-audit-finds-takata-engineers-manipulated-air-bag-test-data (accessed 18 July 2016).

Um, K.-H. and Oh, J.-Y. (2020), "The interplay of governance mechanisms in supply chain collaboration and performance in buyer–supplier dyads: substitutes or complements", *International Journal of Operations & Production Management*, Vol. 40 No. 4, pp. 415-438.

U.S. Customs and Border Protection (2020), "CBP officers seize fake COVID-19 test kits at LAX", [Press release], available at: https://www.cbp.gov/newsroom/national-media-release/cbp-officers-seize-fake-covid-19-test-kits-lax.

Van de Ven, A.H. (1989), "Nothing is quite so practical as a good theory", *Academy of Management Review*, Vol. 14 No. 4, pp. 486-489.

Vaughan, D. (1999), "The dark side of organizations: mistake, misconduct, and disaster", *Annual Review of Sociology*, Vol. 25 No. 1, pp. 271-305.

Voss, C., Tsikriktsis, N. and Frohlich, M. (2002), "Case research in operations management", *International Journal of Operations & Production Management*, Vol. 22 No. 2, pp. 195-219.

Walker, G., Kogut, B. and Shan, W. (1997), "Social capital, structural holes and the formation of an industry network", *Organization Science*, Vol. 8 No. 2, pp. 109-125.

Wathne, K.H. and Heide, J.B. (2000), "Opportunism in interfirm relationships: forms, outcomes, and solutions", *Journal of Marketing*, Vol. 64 No. 4, pp. 36-51.

Wilhelm, M.M., Blome, C., Bhakoo, V. and Paulraj, A. (2016), "Sustainability in multi-tier supply chains: understanding the double agency role of the first-tier supplier", *Journal of Operations Management*, Vol. 41, pp. 42-60.

Williamson, O.E. (1975), *Markets and Hierarchies: And Antitrust Implications*, The Free Press, New York.

Williamson, O.E. (1985), *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*, Free Press, New York, NY.

World Customs Organization (2020), "COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment", [Press release], available at: http://www.wcoomd.org/en/media/newsroom/2020/march/covid_19-urgent-notice-counterfeit-medical-supplies.aspx.

Yamoah, F.A. and Yawson, D.E. (2014), "Assessing supermarket food shopper reaction to horsemeat scandal in the UK", *International Review of Management and Marketing*, Vol. 4 No. 2, pp. 98-107.

Yin, R.K. (2009), *Case Study Research: Design and Methods*, Sage, Vol. 5.

Zaheer, A. and Bell, G.G. (2005), "Benefiting from network position: firm capabilities, structural holes, and performance", *Strategic Management Journal*, Vol. 26 No. 9, pp. 809-825.

Zaheer, A. and Soda, G. (2009), "The origins of structural holes", *Administrative Science Quarterly*, Vol. 54 No. 1, pp. 1-31.

Zaheer, A., Gözübüyük, R. and Milanov, H. (2010), "It's the connections: the network perspective in interorganizational research", *Academy of Management Perspectives*, Vol. 24 No. 1, pp. 62-77.

Appendix

The Appendix is available online for this article.

Corresponding author

Scott DuHadway can be contacted at: duhadway@pdx.edu