Abstract

Problem Definition: Counterfeit parts are a growing and costly problem in various B2B (business-to-business) settings. We have two broad research questions. First, what are the major supply chain drivers of counterfeit risk? In particular, we study how manufacturer-related, distributor-related, and customer-related drivers contribute to counterfeit risk, and quantify the relative impact of each of these drivers. Second, how can counterfeit risk be mitigated? We examine the impact of three operational strategies: increasing flexibility, lead time management, and information sharing in mitigating counterfeit risk.

Academic/Practical Relevance: Existing literature has largely focused on the counterfeit problem in the B2C (business-to-consumer) context, in particular, on why consumers may knowingly purchase non-deceptive counterfeit products and on strategies to prevent such purchases. The problem of deceptive counterfeit products in the B2B (business-to-business) context, where businesses unknowingly purchase counterfeits has been largely understudied in the operations literature. We provide insights on supply chain drivers of these purchases. We add to this literature by introducing the concept of distribution flexibility as a mitigation strategy.

Methodology: We use econometric models to analyze data on 6,905 FPGA (field programmable gate array) parts, made by 19 manufacturers and sold through 37 authorized distributors and 51 unauthorized sources in the 2013-2015 timeframe.

Results: We find that significant increase (positive trend) in lead time, higher price difference between authorized distributors and unauthorized sources, and higher number of customer-driven part changes lead to an increase in the counterfeit risk for the part. We show that increasing distribution flexibility, managing lead time, and sharing information are effective strategies to mitigate counterfeit risk.

Managerial Implications: Our results show specific actions managers can take to mitigate counterfeit risk. We also highlight counterfeit parts as one of the unintended consequences of policy changes that can affect the entire supply chain.

Keywords: supply chain risk, counterfeit electronic parts, FPGA (field programmable gate array), distribution network, operational flexibility, B2B (business-to-business), empirical analysis.
1 Introduction

A counterfeit part is defined as a fraudulent part that is created by manufacturing, altering, distributing, or offering a product or package that is represented as genuine (Defense Federal Acquisition Regulation Supplement, 2018). Counterfeit electronic products have grown to now represent 18% of all seizures, and counterfeit parts in products that pose public health, safety, and security risks have doubled since last year, indicating that the sophistication of counterfeit electronic components have only increased over time (U.S. Customs and Border Protection 2016). Today the economic impact from counterfeit electronic parts is estimated to be approximately $169 billion, second only to counterfeit drugs (Havoscope Global Black Market Information 2016). According to the U.S. Semiconductor Industry Association, counterfeit semiconductors cost the U.S. semiconductor industry an estimated $7.5 billion per year, which translates into nearly 11,000 lost American jobs (Semiconductor Industry Association 2013).

Counterfeit electronic parts are regrettably widespread and pose serious risks to global supply chains, public health and safety, and civilian and military infrastructure. In response to this threat, the U.S. government and industry associations conducted targeted investigations between 2011-2013 to understand how counterfeit parts enter the marketplace (U.S. Senate Armed Services Committee 2011; National Defense Authorization Acts of 2012 & 2014). These reports highlight several vulnerabilities in the electronic component supply chain that allow for entry of counterfeit parts. Those that involve supply chain risk are the focus of our study.

The electronic component supply chain (Figure 1) consists of manufacturers (OCMs – original component manufacturers), distributors, and customers (OEMs – original equipment manufacturers). Over 80% of the sales in this industry happen through the distribution network that consists of both authorized distributors and unauthorized sources (like independent distributors, brokers, and other resellers). A consistent finding across all investigations is that counterfeit parts enter the supply chain when customers purchase parts from unauthorized sources (Government Accountability Office 2012; Semiconductor Industry Association 2013). One of the key drivers for this is the unavailability of authentic parts at the authorized distributors. When parts are unavailable, customers look for alternate, possibly unauthorized, sources. Some of these sources may have procured parts from other resellers and the customer may unknowingly purchase a counterfeit part. As a result, the whole supply chain faces serious consequences from a counterfeit part. For example, Cisco claimed 27 million USD as compensation in false warranty claims in 2011 (Tung 2011). Some part failures at OEMs were wrongly attributed to lack of quality, even though the parts themselves were counterfeit. Cisco had to spend time and resources to determine the cause of failure and (more importantly) suffered a loss of reputation in the market.

In this paper we conduct an empirical analysis of supply chain drivers of counterfeit risk and examine the effectiveness of three operational strategies in mitigating counterfeit risk: increasing distribution
flexibility, managing lead time, and sharing information. Since counterfeit parts enter the supply chain when customers purchase parts from unauthorized sources, we consider all three key supply chain members, the manufacturer, the distributor, and the customer (Figure 1), that may have a hand in creating such incidents and can take actions to prevent them. We have two broad research questions. First, what are the major supply chain drivers of counterfeit risk? In particular, we study how manufacturer-related, distributor-related, and customer-related drivers contribute to counterfeit risk, and quantify the relative impact of each of these drivers. Second, how can counterfeit risk be mitigated? The supply chain risk management literature broadly recommends increasing flexibility, buffering or building redundancies, and aligning incentives and information (e.g., Lee 2004; Sheffi and Rice 2005; Tomlin 2006; Sodhi and Tang 2012). We adopt these to the context of counterfeit parts occurring in the electronic component supply chain and study their effectiveness in reducing counterfeit risk.

On flexibility, we introduce and test the concept of distribution flexibility. We adapt the measure of manufacturing process flexibility developed by Graves and Tomlin (2003) to electronic part distribution. Our measure of distribution flexibility captures the ease with which customers can find an electronic part or a good substitute for it within the authorized distribution network. It is when customers go outside the authorized distribution network that they leave the supply chain vulnerable to counterfeiters. On buffers and redundancies, we focus on the impact of lead time management. The particular metric we use to capture the notion of a lead time buffer is the difference between part lead time and the minimum lead time for a substitute part within the authorized distribution network. A larger buffer in this sense makes it less likely that customers will purchase from unauthorized sources. Finally, with respect to information sharing, we focus on change notifications that OCMs issue to their downstream supply chain partners on upcoming change to the part.

Our empirical analysis focuses on FPGA (field programmable gate array) parts as they often feature in counterfeit incidents (more on them in Section 3.2). We collated information on FPGA parts from multiple private and public databases such as SiliconExpert, Electronic Component Industry Association (ECIA), individual manufacturer and distributor websites, and private repository of counterfeit reports (Gamma) to create a unique dataset of 6,905 FPGA parts made by 19 manufacturers and sold through 37 authorized and 51 unauthorized distributors. This dataset includes counterfeit reports on each authentic part, its authorized distribution network (including inventory, lead time and price at these distributors), its unauthorized sources, any change notifications on part changes shared by manufacturers with downstream supply chain members, and part details (part characteristics and part changes). We analyze our research questions using a probit model with sample selection. Our main findings are:

1. high-value parts are at an increased risk of being counterfeited;
significant increase (positive trend) in lead time, higher price difference between authorized
distributors and unauthorized sources, and higher number of customer-driven part changes lead to
an increase in the counterfeit risk for the part;

(3) increased distribution flexibility significantly reduces counterfeit risk (this flexibility is even more
valuable when there is a higher positive trend in the lead time for the part compared to other parts
in the network);

(4) increased information sharing and increased lead time buffer reduce counterfeit risk; and

(5) increased distribution flexibility complements the effect of information sharing and lead time buffer
in reducing the overall counterfeit risk for the part.

To the best of our knowledge this is the first paper that empirically examines supply chain drivers of
counterfeit risk, and provides evidence for flexibility in the distribution network as a counterfeit risk
mitigation strategy. Our results contribute to the academic literature in two ways. First, existing literature
has largely focused on the counterfeit problem in the B2C (business-to-consumer) context, in particular, on
why consumers may knowingly purchase non-deceptive counterfeit products and on strategies to prevent
such purchases (Qian 2014; Cho et al. 2015). We add to this literature by analyzing the problem of deceptive
counterfeit products in the B2B (business-to-business) context, where businesses unknowingly purchase
counterfeits, and we provide insights on supply chain drivers of these purchases (Semiconductor Industry
Association 2013). Second, operational flexibility has been extensively studied in operations management
as an effective strategy to mitigate the impact of demand-supply mismatches (e.g., Jordan and Graves 1995;
van Mieghem 1998, 2007; Graves and Tomlin 2003, Sodhi and Tang 2012). We add to this literature by
introducing distribution flexibility and showing that higher distribution flexibility mitigates counterfeit risk.

Our results have implications for both managers and policy makers. First, we provide insights on the
supply chain drivers of counterfeit risk. We find that when manufacturers are not adequately prepared to
undertake large scale customer-driven changes, it can lead to a significant increase in lead time and
temporary shortages in the supply chain, thus increasing counterfeit risk. Second, we quantify the
effectiveness of distribution flexibility, lead time management, and information sharing as strategic levers
for counterfeit risk mitigation, and show that they complement each other. We find that adding one
additional distributor to parts that have 2 or less distributors (without increasing the overall inventory level)
reduce counterfeit risk by 11.14% and increase effectiveness of information sharing by an additional
9.81%. For parts with high average lead time or positive trend in lead time, increase in distribution
flexibility, higher lead time buffer, and increased information sharing help lower counterfeit risk by an
additional 4.79%, 2.32%, and 3.71% respectively. Finally, our results also have implications for policy
makers. We show that when multiple members in the supply chain have to make large scale changes in
order to comply with new environmental regulations, this can create temporary shortages in the supply
chain. Our results show that this provides an opportunity for counterfeit (non-compliant) parts to enter the supply chain and policy makers must take steps to prevent such unintended consequences.

2 Literature review

Although there is limited research on counterfeit electronic parts, the problem of counterfeit products in general has been studied in marketing and operations management, but almost exclusively in B2C contexts. Counterfeit products are classified as deceptive and non-deceptive. In the case of deceptive counterfeits, also called blur counterfeits, the consumer is unaware or unsure of the fact that she is purchasing a counterfeit, while in the case of non-deceptive counterfeits, consumers can distinguish the product from the brand-name or authentic product at the time of purchase (Grossman and Shapiro 1988; Bian and Moutino 2009; Cho et al. 2015). Much of the existing literature on counterfeits in B2C settings focuses on the problem of non-deceptive counterfeits, examining the reasons why consumers purchase them and various ways by which firms can prevent or choose to accommodate them. On the demand side, the literature shows that price, attitudes towards big-brand companies, and the need for status signaling are some of the key factors driving purchase of counterfeit products (Cordell 1996; Bian and Moutino 2009; Qian 2014). On the supply side, counterfeits are more likely to enter the market when they bear a high resemblance to genuine products, they can claim a high profit margin, and there is relatively weak IPR (intellectual property rights) enforcement (Siu et al. 2010, Tse et al. 2010, Qian 2014). Effective strategies against counterfeit products include differentiating on price and quality (Cho et al. 2015), expanding the product line by introducing peripheral products (Yildirim et al. 2017), and investing in self-enforced IPR by opening licensed stores and monitoring the market for counterfeit goods (Qian 2014). We contribute to this literature with an empirical analysis of the problem of deceptive counterfeits in a B2B setting. We highlight the role of supply chain factors in driving the occurrence of counterfeit parts and explore the effectiveness of three specific operational strategies to mitigate them.

The problem of product flows through unauthorized distribution channels can be mitigated through use of appropriate price discounts and price-dependent quantity discount contracts (Hu et al. 2013; Ahmadi et al. 2015). Just as counterfeits steal demand from genuine products, these unauthorized channels compete with the authorized channel for sales to customers, but the underlying assumption in the models developed in extant literature is that the products offered in these unauthorized channels are still genuine products. Also, this body of work exclusively focuses on B2C contexts. We highlight counterfeit risk as an additional risk associated with purchase of products from unauthorized channels and we conduct our empirical analysis in a B2B setting.

Counterfeit products are also related to product adulteration in the supply chain, where poor-quality or non-conforming products might be propagated. Traceability and testability of the products and transparency in the supply chain have been advocated as some of the critical factors in ensuring safety in the supply chain.
There has also been recent work around effective contractual mechanisms to ensure quality of products (Starbird 2001; Chao et al. 2009), use of inspection mechanisms to test for quality (Balachandran and Radhakrishnan 2005; Babich and Tang 2012), and effectiveness of process audit and contingency payments to screen suppliers (Chen and Lee 2014). While product adulteration literature essentially looks at malfunctioning of the ‘authorized’ supply chain, the counterfeit problem can occur even without such malfunctioning since counterfeit products typically originate from outside the authorized channels. Our contribution to product adulteration literature is indirect: Some of the mechanisms and supply chain factors that increase the chances of counterfeit products entering the supply chain might be operational in how product adulteration occurs, e.g., a third-tier supplier using a non-compliant paint for toys because it is cheaper.

3 Industry background, research setting, and FPGA data

In this section, we first provide an overview of the supply chain structure for integrated circuits (ICs), explain in detail the distribution network for ICs, and how counterfeit parts enter this supply chain. Next, we detail our major data sources on FPGA parts (a type of IC) and describe the sample that we use for our empirical analysis.

3.1 Supply chain for integrated circuits

Integrated circuits, which are microelectronic semiconductor devices comprising of many interconnected transistors and other components, account for 82.1% of global semiconductor revenue and are used in a variety of devices including computers, audio and video equipment, automobiles, medical and industrial equipment, and public safety and military systems (IBISWorld 2014). In the IC supply chain, the manufacturing process (wafer fabrication) is the most time consuming and resource intensive process (Brown et al. 2000). Most IC manufacturers (OEMs) today operate on a ‘fabless’ mode, i.e., they outsource the wafer fabrication and assembly processes to foundries. On average, the lead time for these processes is 3-4 months, and can be longer when there are disruptions to the production process. Due to this, the manufacturers rely heavily on their distribution network to hold inventory and meet customer demand. For instance, Xilinx meets more than 70% of the demand through its distributors (Brown et al. 2000). Further, electronic component distributors perform several value-add functions beyond traditional warehousing and inventory management. These include “demand generation”, wherein distributors actively participate in the customer’s design and prototype phases and try to secure a “design win” for the part, and provide technical expertise on part compatibility for the customer’s system. It is not uncommon for customers to take their complete Bill-of-Materials to the distributor and allow them to suggest the right set of parts (and manufacturers) to be used in their system (Kickham 2011). Thus, we observe that a major portion of IC sales occur through the distributors in the supply chain. Hence, the distribution network plays a key role in ensuring that there is enough supply to meet demand.
The distribution of parts occurs via authorized distributors (i.e., distributors who are certified by the manufacturer to carry the parts) and unauthorized sources, which include independent distributors, other resellers, and brokers, who are not certified by the manufacturer but are still allowed to carry and sell the parts. Unauthorized sources typically buy the part from the OCM, contract manufacturers, authorized distributors, and other sources ahead of time and stock them for resale. One of the key differences between authorized distributors and unauthorized sources is the level of product support they receive from the manufacturer. Authorized distributors have special agreements with the manufacturer to access specification guarantees; are provided with warranty support, engineering and failure data analysis of the parts; and get preferred pricing and inventory allocation. These distributors are regularly audited by the manufacturers to make sure they adhere to quality standards on handling and storage of parts. Similar to the automotive industry, many manufacturers implement a push system that allocates inventory to distributors. Authorized distributors are further allowed to take a fraction of the volume (can be as high as 90%) back from the customers as well as return unsold inventory to the manufacturers and receive credit for the returned parts (U.S. Department of Commerce 2010). In this way, authorization protects the distributor from the downside of having excess inventory. Unauthorized sources on the other hand, purchase and stock inventory of parts in anticipation of customer demand. Their sources for purchase include excess inventory from customers (e.g., OEMs, system integrators, etc.), production overruns from contract manufacturers, and surplus from other distributors or manufacturers. They are not audited by manufacturers but may independently perform quality assurance on parts that are purchased. Anecdotal evidence suggests that it is difficult to guarantee authenticity of the part outside the authorized distribution network. For example, a recent survey of counterfeit parts found that more than 80% of counterfeit parts enter the supply chain when they are purchased from an unauthorized source (U.S. Department of Commerce 2010; Government Accountability Office 2012).

3.2 Research setting

We conduct an empirical analysis of the supply chain drivers of counterfeit risk and effectiveness of mitigation strategies for FPGA parts. An FPGA part is an IC that is designed to be configured by a customer. FPGAs can be further classified into 7 different part-categories: SRAM (static random access memory), Fuse and Antifuse, PROM/EPROM/EEPROM (programmable read only memory, erasable and electrically erasable programmable read only memory), and Flash Memory.

Counterfeit FPGA parts are a major concern for the electronics industry for the following reasons. First, ICs form a major portion of counterfeit electronic part reports in recent years (87% in 2015), and among ICs, counterfeit FPGA parts have been on a consistent rise in the last 5 years (up 48% in 2011-2015 period). Second, there are a limited number of FPGA manufacturers and, for these firms, FPGA parts form a significant part of their business. Hence, counterfeit parts pose a significant threat for these firms.
example, Xilinx and Altera are the top two manufacturers of FPGA and are also the most frequently mentioned names in counterfeit reports. As a result, these firms are incentivized to invest in anti-counterfeit measures for these parts. Third, FPGAs are widely used in the electronics industry, ranging from consumer electronic products like laptops and cell phones, industrial systems like HVAC systems, and military applications like missile systems. Counterfeit FPGA parts can lead to malfunctioning or failure of these systems, resulting in high cost of repair and re-work, and even loss of life in some instances. Thus, identifying and evaluating the effectiveness of operational strategies to prevent counterfeit FPGA parts would have a significant economic impact on the electronics industry. Our data covers the distribution network of active FPGA parts marketed in the US.

3.3 Data sources

Part characteristics: We obtained part-level data on part characteristics from SiliconExpert. SiliconExpert is a private company that provides information on electronic component distribution to its customers through a membership fee. SiliconExpert's customers include: leading commercial and government OEMs, top-tier authorized distributors, contract manufacturers and component suppliers. We collected information on the introduction date, options for the part from the same firm, and substitutes for the part from other firms from this database.

Distribution network: We collected information on the authorized distributors, inventory (out-of-stock or units available), lead time for delivery, and price of the part at each distributor from the SiliconExpert database. We augmented missing information from the Electronic Component Industry Association (ECIA) website and from the individual distributor websites. We collated information across these sources to create a distribution network for each set of substitutable parts. In addition to this, we manually collected information from other third-party websites on the number of unauthorized sources that list the part as “available” and the quoted price at these sources.

Product datasheets and change notifications: We obtained product datasheets and product change notifications for each part from each manufacturer’s website. The datasheets contain the technical details of each part including the part-family, electrical data operating range, package information, and manufacturing process. As an example, consider the part “XC6SLX9-2CSG225C” made by Xilinx. It belongs to the “XC6SLX9” part-family (a.k.a. Spartan-6 Family) and the SRAM part-category. The product datasheet lists the number of logic cells, the voltage, power, and speed specifications, clock and configuration details, and pin and package information. Parts within a part-family are generally considered as functional substitutes. Each part-family is unique to a manufacturer. We used the functionality and package information in the datasheet to group parts from different manufactures under a part-category and to validate the list of substitute parts across manufacturers obtained from SiliconExpert. We used the datasheets to track material, process, and functionality changes that were driven by the customer during the
time period of our analysis. We combined this information with press releases from the manufacturer’s website as well as from the Lexis-Nexis website to classify the changes as *internal* (initiated by the manufacturer in anticipation of change in industry or customer requirements) or *external* (initiated by the customer or necessitated by regulation with a specific deadline for compliance). The change notifications included information on the date of notification and the reason for the change. Matching information from the product datasheets and change notifications, we collated a list of internal and external changes to the part and if notifications were issued about these changes during the time period of our analysis.

*Counterfeit reports:* We collected counterfeit reports from a third-party website *Gamma* (name is disguised to maintain confidentiality). Each report included information on the date of filing, the part that was counterfeited (part number and manufacturer), and price of the counterfeit part. Unlike other industries (e.g., apparel or software purchases) customers do not intentionally buy counterfeit electronic parts. Instead, the underlying assumption is that the parts are genuine and the quoted price is the price for the genuine part. Post-purchase, customers conduct a quality inspection of these parts, at which point counterfeit parts (if present) are discovered. Since there are heavy penalties associated with use of a counterfeit part, customers tend to take these activities seriously and file counterfeit reports accurately with *Gamma*. Hence, we use the counterfeit reports as a proxy for counterfeit part purchases.

### 3.4 Data description

Authorized distributors report inventory and lead time information to SiliconExpert on a half-yearly basis. We collected the latest available inventory and lead time information from SiliconExpert and ECIA for the year 2013 and 2014 for these parts. We combined this with information on changes to the part and change notifications that were issued for these parts for the year 2013 and 2014 from product datasheets, manufacturer websites, and Lexis-Nexis websites to create a master database on part information and the distribution network. Next, we matched the part information with counterfeit reports from *Gamma*. Based on the report date, we classified the counterfeit reports as “prior counterfeit reports” (i.e., the reports issued before the release of inventory and lead time information) and “counterfeit reports” (i.e., reports issued after the release of inventory and lead time information). Since we only consider the latest available information update on inventory, lead time, product datasheets, and change notifications, we have a single cut-off point for each part. The timeline we use to create our sample is explained graphically in Figure 2. For example, consider a part with the following information updates: Last available distributor and inventory information in May 2014, last change notification issued in January 2014, and last documented change to the part from the product datasheet in March 2014. We use May 2014 as the cut-off date and check if there was a counterfeit report in the 6-month period after this cut-off date (we check for robustness across other time periods see Section 7). After combining information from the above data sources and removing observations for which we had incomplete data on our key variables (inventory, lead time, and price), we
have a sample of 6,905 parts across 19 manufacturers, 37 authorized distributors, and 51 unauthorized sources. In this sample, 1,125 parts had at least 1 counterfeit report.

4 Supply chain drivers of counterfeit risk

The electronics industry has seen a significant shift towards a global supply chain over the last decade. This shift is even more pronounced in the context of FPGA parts, where most of the production is outsourced to a few foundries located outside the US and the production process is characterized by long lead times and capacity constraints. At the same time, due to rapid advances in IC technology, firms continue to introduce new products at a faster rate in order to remain competitive in the marketplace. These two trends together expose firms in the supply chain to high levels of both supply and demand uncertainty (Fisher 1997; Lee 2002). Further, high demand for FPGAs attracts many unauthorized sources of supply. As it is hard to verify the authenticity of FPGA parts in general, increase in unauthorized sources of supply and price competition between the authorized distributors and unauthorized sources lead to high levels uncertainty in the distribution of these parts.

Therefore, high supply, distribution, and demand uncertainty render the FPGA parts extremely vulnerable to supply chain risk related to counterfeiting. We organize the drivers of counterfeit risk for FPGA parts under the three key nodes of FPGA supply chain: the manufacturer, the distributor, and the customer (Figure 1).

Manufacturer-related drivers of counterfeit risk

Manufacturer-related drivers pertain to risk events on the supply side that include supplier failure as well as unexpected changes in supply cost, delivery, quality, or reliability (Chopra and Sodhi 2004; Tomlin 2006; Sodhi and Tang 2012). Supplier failure can lead to high lead times and unreliable deliveries (Hendricks and Singhal 2005; Tomlin and Wang 2012). This is further exacerbated when manufacturers do not have the flexibility to modify supplier commitments in response to shortfalls – a common occurrence in the electronics industry (Brown et al. 2000; Sheffi 2005; Tomlin and Wang 2012). Further, in the event of a supply disruption, low levels of operational buffer (maintaining additional inventory or additional capacity at an alternate supplier) could lead to a rapid increase in the lead time for the part during the period of disruption. Such unanticipated changes in cost and delivery could lead customers to explore alternate sources of supply (Government Accountability Office 2012).

We examine the effect of manufacturer-related drivers through variables that capture the extent of shortage in the distribution network, the average lead time, and the trend in lead time for the part, which are all under the part manufacturer’s purview. Based on the above, we hypothesize that:

H1: Parts that experience shortages, a high lead time, or a higher positive trend in lead time have higher counterfeit risk.
Distributor-related drivers of counterfeit risk

Distributor-related drivers relate to distribution practices that encourage customers to purchase from unauthorized sources in the market. Prior literature has shown that manufacturers are more likely to manage pricing by controlling the number of distributors and inventory in the channel, more so when they have relatively high bargaining power in the channel (Frazier and Lasser 1996; Iyer and Boas 2003; Iyer et al. 2007; Draganska et al. 2010). For products that have a long life-cycle and are in high demand, like pharmaceuticals and electronic components, such practices may inadvertently encourage the emergence of unauthorized channels of distribution where products are often sold at lower prices but without the service and warranty support available in the authorized channel (Hu et al. 2013, Ahmadi et al. 2015). Since these unauthorized channels obtain the products from other resellers, and not directly from the manufacturers, they are more vulnerable to counterfeits even when they have an inspection mechanism in place (Roth et al. 2008; Babich and Tang 2012). Often, these unauthorized sources provide heavy price discounts to steal business away from authorized distributors (Government Accountability Office 2012). This, in turn, may motivate customers to purchase the part from unauthorized sources even if it is still available at authorized distributors and thus increase the risk of counterfeit parts entering the supply chain.

We examine the effect of distributor-related drivers through variables that capture the number of unauthorized sources and the price difference between the authorized distributors and unauthorized sources for the part. Hence, we hypothesize that:

\[ H2: \text{Parts that have a higher number of unauthorized sources and a higher price difference between authorized distributors and unauthorized sources have higher counterfeit risk.} \]

Customer-related drivers of counterfeit risk

Customer-related drivers relate to (1) change in demand for the part due to change in underlying technology and customer preferences for the part, and (2) change to the business ecosystem through introduction of new environmental requirements or legislation that influence customer demand. Such changes could lead to increased uncertainty in long-term demand for the part (Sheffi 2005).

In cases where most of the production is outsourced, manufacturers may reduce capacity in anticipation of these changes ahead of time to save on overcapacity and commitment costs (Hendricks and Singhal 2011). This could create shortages for the existing products in the supply chain and lead customers to look for alternate sources of supply to tide over the temporary shortages. Environmental regulations and compliance requirements can also have a long string of unintended consequences on both the supply and the demand side. These include shrinking of the supply base (Lee 2010), imposing external changes on the manufacturer that could entail significant changes to a firm’s operations (Corbett and Klassen 2006; Plambeck 2013), and changing demand for the products (Zhang et al. 2017). In order to comply with these
regulations, customers further down in the supply chain may need to dispose older parts that are functional and active but become non-compliant due to a change in regulations. Often these parts are sold on the secondary market to gain some salvage value. When counterfeiters gain access to such parts, they can easily pass them along as genuine parts by simply changing the label and marking them as compliant (U.S. Department of Commerce 2010). As a result, these customer-related drivers can lead to an increase in supply of counterfeit parts at the unauthorized sources.

We examine the effect of customer-related drivers on counterfeit risk through variables that capture the number of internal and external changes to the part that are driven by a change in customer requirements. Internal changes are proactive and their typical purpose is to meet additional demand, whereas external changes are reactive, usually to a mandated or legally required rule (they are explained in more detail in Section 3.3). Based on the above, we hypothesize that:

\[ H3: \text{Parts that undergo higher number of internal and external changes have higher counterfeit risk.} \]

5 Empirical analysis of supply chain drivers of counterfeit risk

In this section we first explain our main data variables, the methodology to test the above hypotheses, and then summarize our main results on the supply chain drivers of counterfeit risk.

5.1 Data variables

a. Dependent variable indicating counterfeit risk:

Counterfeit Reports \((CR_i)\) – This is a binary variable coded as 1 if a counterfeit report exists in the six-month period after the cut-off date for part \(i\), part-family \(j\), part-category \(c\), manufactured by firm \(f\). Testing a FPGA is a complex process and counterfeit detection is only a part of the overall inspection process. Based on our conversations with Gamma and representatives at OEMs it can take between 1-3 months from purchase of a part to filing a report with Gamma. We choose a six-month period to give enough time for a part to be tested and a counterfeit report (if the part is a counterfeit) to be filed with Gamma. We do a robustness check around different time periods in section 7. To keep the notation simple, we only retain the subscript \(i\) for part-related variables.

b. Independent variables on supply chain drivers:

Average lead time, trend in lead time, \((L_i, L_{T_i})\) – These are the average lead time and trend in lead time for the part respectively. The average lead time is the average over all authorized distributors. We were able to also obtain historical lead time information from SiliconExpert. For the parts in our sample, this would be the last 5 observations on lead time. Hence, we calculate the trend in lead time \((L_{T_i})\) as the slope in average lead time over the past 5 observations.

Internal and External Changes \((IC_i, EC_i)\) – These are the log of the number of internal and external changes made to the part, respectively.
Price \((P_i, PD_i)\) – These are the price of the authentic part at the authorized distributor and the price differential for the part as quoted by the authorized distributor(s) and the unauthorized source(s). The price at the authorized distributors show negligible variation during the time period of our study. The price at the unauthorized source is the average of prices quoted by all the unauthorized sources. The price differential is normalized by the price at the authorized distributor; it equals \((P_i - \text{average of prices at unauthorized sources}) / P_i\), and thus represents the average percentage discount that unauthorized sources give over the authorized-channel price.

Shortages \((S_i)\) – This is the extent of shortage for part \(i\). It is operationalized as the ratio of number of authorized distributors that are out-of-stock to the total number of authorized distributors for part \(i\).

Unauthorized sources \((U_i)\) – This is the number of unauthorized sources that report part \(i\) as “available.”

c. Controls:

Popular part \((PP_i)\) – This is a binary variable that is coded as 1 if the part is described as a popular part in the SiliconExpert database, 0 otherwise. We do not have demand information for each part in our data. SiliconExpert uses the binary variable \(PP_i\) to indicate if historically a high demand (compared to other parts in the same part-category) has been observed for the given part. Hence, we use this information to control for demand effects in our analysis.

Prior counterfeit reports for part-category \((PC_{cf})\) – This is the count of prior counterfeit reports for the part-category from the same firm. We use the logged variable in our analysis.

Years since introduction \((Y_i)\) – This is the number of years since the part was introduced in the market. We normalize this variable with the average life for all parts in the part-family.

Fixed effects \((W_{fcn})\) – These include the firm fixed effect, the part-category fixed effect, and the distribution network fixed effect.

Summary statistics for our main data variables are provided in Table 1.

5.2 Empirical specification

In order to econometrically model the relation between counterfeit risk and the supply chain drivers, we need to address two issues. First, a counterfeit part enters the supply chain when a counterfeit part exists for the genuine part. It is possible that some parts are more easily counterfeited than others which means that they are more likely to be available for purchase from unauthorized sources. This introduces a selection bias that needs to be controlled in our econometric model. Second, counterfeit risk for a part is a latent variable since we only observe counterfeit reports for the parts, not the underlying risk. To address these two issues, we use a probit model with sample selection (Greene 2008) that builds on Heckman’s (1979) sample selection model. In brief, this procedure involves the joint maximum-likelihood maximization of: (1) a selection equation that identifies when the dependent variable is observed; and (2) an outcome equation.
that identifies the binary outcome of the dependent variable. Next, we discuss the selection and outcome equations in detail.

5.2.1 Selection equation
In our setting, the selection equation identifies when counterfeit parts exist for the corresponding genuine part. A unique characteristic of counterfeit electronic parts is that it can be passed along as a genuine part as long as it is “close enough” in appearance and functionality to a genuine part. Parts that belong to a part-family often share similar physical characteristics and only have minor variations in their functionality. For example, in the part-family “XC6SLX9” from the Spartan-6 LX FPGA product range, there are almost 11 active parts that have similar physical characteristics and performance but differ only in the number of logic cells available to program at the user-end. However, it is not until the time of actual deployment that the number of available logic cells can be determined. In this context, a counterfeit part can be passed along as a genuine part for any of the parts within this part-family by simply promising the requested number of logic cells. As has been often reported in many test reports, this type of counterfeiting is only detected when the parts are put through rigorous destructive functional tests. Hence, for the first-stage, we use a binary variable $C_j$ that captures the probability that a part-family is counterfeited. This variable is coded as 1 if counterfeit reports exist for the part-family $j$ in the six-month period prior to our cut-off date. Anecdotal evidence and prior literature suggest that counterfeiters often target parts that are likely to be more profitable (Gao et al. 2017, Pun 2017). In our context, part characteristics like high demand, high margin, and ease of imitation could influence the production of counterfeit parts. Hence, we use the following specification for the selection equation:

$$C_j = \beta_0 + \beta_1 Y_j + \beta_2 \bar{P}_j + \beta_3 \bar{L}_j + \beta_4 \bar{P} \bar{L}_j + \beta_5 P_{cf} + \beta_6 W_{fc} + \epsilon_{jcf}$$

(1)

In the above equation, $C_j$ indicates whether there exist counterfeit reports for part-family $j$ prior to the cut-off date for part-family $j$, and $Y_j$, $\bar{P}_j$, $\bar{P} \bar{L}_j$, $\bar{L}_j$ are the average years since introduction, average price, part popularity and average lead time over all parts in the part-family, respectively. We make sure to only use information prior to the counterfeit report while constructing these variables. The above selection equation is common across all specifications of the outcome equations. The outcome equation identifies whether there exist counterfeit reports for part $i$ in the six-month time window after the cut-off date.

5.2.2 Outcome equation
To test our hypotheses in Section 4, we represent counterfeit risk for a part as function of the variables that represent the manufacturer-related drivers (shortages, average lead time, and trend in lead time), distributor-related drivers (number of unauthorized sources, price difference), and customer-related drivers (number of internal and external changes) in the supply chain.

To capture the impact of lead time we use two variables, the average lead time and the trend in lead time for the part. The lead time for parts can vary widely across different part categories depending on the
underlying production technology and the structure of the supply chain for these parts. For example, the average lead time for programmable read only memory FPGAs is 2.1 weeks while the average lead time for reprogrammable memory FPGAs is 7.5 weeks. To enable comparison across different parts, we measure the lead time of the part relative to all other parts within the distribution network, i.e., relative to all other parts that are substitutes to it. We divide the average lead time for all substitutable parts into quartiles ($L_Q_i$ captures the quartile information). Parts belonging to the top quartile would have relatively higher lead time compared to other substitutable parts. Similarly, we divide the trend in lead time for parts within the distribution network into quartiles ($L_T Q_i$) where the top quartile indicates parts that have a relatively high trend in lead time compared to all other substitutable parts.

Finally, we also include controls for price of the part, prior counterfeit reports for the part -category, years since introduction, and if the part is a popular part, as well as part-category, firm, and network fixed effects. We use the following specification for the second stage:

$$CR_i = \alpha_0 + \alpha_1 S_i + \alpha_2 L_Q_i + \alpha_3 L_T Q_i + \alpha_4 P_i + \alpha_5 P_{Di} + \alpha_6 U_i + \alpha_7 EC_i + \alpha_8 IC_i + \rho_1 PC_{cf} + \rho_2 Y_i + \rho_3 PP_i + \rho_4 W_{fcn} + \varepsilon_i$$

$\varepsilon_i$ represents the error term. We use clustered standard errors at the part-category level in all our analysis. Note that both selection equation (1) and outcome equation (2) are probit models, and we have suppressed their full functional form for ease of exposition throughout the paper. (In both cases, the binary variable on the left-hand-side is considered 1 when the right-hand-side is strictly positive, and 0 otherwise.) Since both $C_j$ and $CR_i$ are binary variables, we use the “heckprobit” routine in STATA to estimate the models. The Variance Inflation Factor (VIF) statistics for all variables in our model were less than 10 – indicating that we do not have any significant multicollinearity.

### 5.3 Estimation results

The results of our estimation of models (1) and (2) are shown in columns S1 and C1 of Table 2. For the manufacturer-related drivers, we find the coefficient for the top quartile for lead time ($L_Q_i; \alpha_2$) and top two quartiles for trend in lead time ($L_T Q_i; \alpha_3$) to be positive and significant ($p<0.05$); other quartiles are not significant. This indicates that parts that have a relatively high lead time tend to be more vulnerable to supply-related problems and have a higher risk of being counterfeited. A higher positive trend in lead time for the parts exposed to supply-related problems further increases the counterfeit risk. We do not find the extent of shortages ($S_i; \alpha_1$) to be significant. Thus, we find partial support for H1.

For the distributor-related drivers, we find that the coefficients for both price differential ($P_{Di}; \alpha_5$) and the number of unauthorized sources ($U_i; \alpha_6$) to be positive and significant ($p<0.05$). This indicates that wide availability of the part from unauthorized source(s) at an attractive price increases the counterfeit risk. Hence, we find full support for H2.
For the customer-related drivers, we find that the coefficient for number of external changes ($EC_i; \alpha_7$) is positive and significant ($p<0.001$) while the coefficient for number of internal changes ($IC_i; \alpha_8$) is not significant. In case of internal changes, many of them are proactive changes taken by the manufacturer in anticipation of increase in demand (e.g., building additional capacity), are planned in advance, and carried out in a phased manner. This reduces the impact of such changes on the normal production and delivery of parts and as a result they do not cause major delays or shortages. Hence, we do not find internal changes to be significantly associated with counterfeit risk.

The impact of external changes on the other hand is different. External changes could be a result of a change in the underlying technology as requested by the customer or a change in industry demand as necessitated by environmental regulations. For heavily engineered parts like FPGAs, it takes considerable amount of time and resources to qualify a new material or production process. When manufacturers do not have enough advance information on the upcoming change, there can be delays in finding the right material or supplier. As a result we observe external changes to have a significant impact on counterfeit risk. Thus, we find partial support for H3.

6 Operational strategies to mitigate counterfeit risk

There is a rich literature in operations management on effective strategies to mitigate supply chain risk. They can be broadly clustered around three ideas: (1) building flexibility in the supply chain; (2) building buffers against shortages arising from supply-demand mismatches; and (3) facilitating close communication and cooperation among supply chain partners to reduce the impact of supply chain risks (e.g., Lee 2004; Sheffi and Rice 2005; Tomlin 2006; Sodhi and Tang 2012). We leverage these to develop specific operational strategies to mitigate counterfeit risk. They include building flexibility in the distribution network, managing lead time of parts, and sharing information with downstream supply chain partners. Below, we explain each of them in detail, quantify their individual impact on counterfeit risk in the FPGA supply chain, and test if these strategies substitute or complement one another.

6.1 Building distribution flexibility

Building flexibility in the supply chain is one of the recommended strategies to mitigate the negative impact of an increase in supply chain risk (Lee 2004; Sheffi and Rice 2005). It takes a variety of forms, including sourcing flexibility - ability to source from an alternate or backup supplier (Tomlin 2006; Tomlin and Wang 2012); production flexibility - ability to shift production from one product or plant to another in response to customer demand (Jordan and Graves 1995; Swaminathan and Tayur 1998; Moreno and Terwiesch 2015), and process flexibility - ability to re-allocate processing resources in a multi-stage supply chain across products (Graves and Tomlin 2003).

In an in-house production environment, increase in production flexibility has been shown to lead to lower inventory levels (Fine and Freund 1999; Cachon and Olivares 2010) while continuing to achieve the
same level of robustness (Simchi-Levi and Wei 2015). In a similar manner, when production is outsourced and there is very little production flexibility with the supplier (as with OCMs in the IC supply chain), manufacturers can leverage flexibility in the distribution network to satisfy customer demands by redeploying products across distributors through transshipments or directly fulfill customer demands from alternate distributors in the network (Sheffi and Rice 2005). We call this distribution flexibility. In the rest of this subsection, we explain how we calculate flexibility in the distribution network.

We adopt the manufacturing process flexibility measure of Graves and Tomlin (2003) to our electronic parts distribution context. (We keep their notation to the extent possible and, henceforth, refer to their work as GT.) Take \( I \) substitutable parts – possibly from multiple manufacturers – carried in \( J \) authorized distributors. Let \( A \) denote the set of arcs representing part-distributor links (akin to GT’s product-plant links); distributor \( j \) carries part \( i \) if and only if \( (i,j) \in A \). Corresponding to each arc, let \( x_{ij} \) be the units of part \( i \) inventory that distributor \( j \) has, which can be zero (we observe these part inventories in the data).

Each distributor then has a total inventory of \( c_j = \sum_{i,j} x_{ij} \), which is analogous to GT’s plant capacities. Let \( \bar{c} = \sum_j c_j / I \) be the average inventory, which reflects an equal-share allocation of total “capacity” among the parts. Define two more sets: \( P(i) = \{j: (i,j) \in A\} \) is the set of distributors that carry part \( i \), and \( P(M) = \bigcup_{i \in M} P(i) \) is the set of distributors that carry some part(s) in \( M \).

We are now ready to define a flexibility measure for each part, for every subset of parts, and for the distribution network defined above for a given set of substitutable parts. Part distribution flexibility is defined as

\[
g_i \equiv \frac{\sum_{j \in P(i)} c_j - \bar{c}}{\bar{c}} = \frac{\sum_{j \in P(i)} c_j}{\bar{c}} - 1 \quad (3)
\]

where \( \sum_{j \in P(i)} c_j \) is the total inventory directly available to satisfy the demand for part \( i \) – available in the sense of providing part \( i \) itself or a substitute for it – in the distributors that carry part \( i \). The measure, therefore, captures the excess inventory available to part \( i \) relative to an equal-share allocation of total inventory among the parts. A larger \( g_i \), in other words, makes it easier for the customers of an authorized distributor looking for part \( i \) to find it or to find a good substitute for it.

The distribution network flexibility is defined as

\[
g \equiv \min_M \{g(M): |P(M)| < J\} \quad (4)
\]

which is the minimum part-group flexibility over all part subsets that do not have access to all of the inventory. If all parts have access to all of the inventory, which GT calls total flexibility, their convention is to set the distribution network flexibility to \( g = I - 1 \) (this is not something we ever observe in the data).

To sum up, for each set of substitutable parts (possibly from multiple manufacturers), we define the distribution network with a bipartite graph and calculate the flexibility measures above – for each part and
for this distribution network (Figure 3). These measures capture the excess inventory available to a group of parts relative to an equal-share allocation of total inventory among all the parts. As such, higher \( g \) values reflect the ease with which a customer can locate a part or a substitute for it in the distribution network.

Part distribution flexibility is a relative measure. It stays the same if one scaled up or down the part inventories (multiplied all of them by a constant). Moreover, increasing the inventory of part \( i \) at distributor \( j \) not only raises the \( g \)-value for parts that share distributor \( j \) with part \( i \), but also lowers the \( g \)-value for the remaining parts. To illustrate this, consider a simple four-part four-distributor example with a distribution network structure shown in Figure 3(b), which GT terms “one complete chain” (p. 908). Suppose all part inventories are 10 units each (for each part in each distributor that carries it), i.e., \( x_{ij} = 10 \) and \( c_j = \bar{c} = 20 \). The part distribution flexibility measures \( (g_1, g_2, g_3, g_4) \) are equal to 1. If we were to have 20 additional units of part 1 inventory in distributor 1 \( (x_{11} = 30) \), then \( g_1 \) and \( g_4 \) would rise to 1.4, whereas \( g_2 \) and \( g_3 \) would drop to 0.6. The reason for the drop is that, in relative terms, parts 2 and 3 are now harder to obtain as they have access to a smaller share of the total (substitutable) inventory.

Distribution network flexibility is generally higher for distribution networks with more links – those that are more flexible. To illustrate this without the confounding effect of inventory, we offer two simple examples. First, consider the same network as in the previous example, and remove the P4-D1 link (resetting \( x_{44} = 20 \) to maintain the same total inventory). The resulting distribution network is shown in Figure 3(a) and the distribution network flexibility becomes \( g = 0.5 \), reflecting a less flexible distribution network. Second, consider adding one more link from each of the four parts as shown in Figure 3(c). Again, the total inventory is kept the same by leaving the existing \( x \)’s the same and setting the new ones to zero \( (x_{13} = x_{24} = x_{31} = x_{42} = 0) \). The distribution network flexibility doubles \( (g = 2) \). Note that at least 4 new links are needed to raise the distribution network flexibility from its original value of 1.

One final observation is in order: All networks that we observe (in our data) are connected graphs, or “chains” in the jargon of Jordan and Graves (1995). That is, adopting their description (p. 580) to our context, no part in a chain is distributed by a distributor from outside that chain, and no distributor in a chain distributes a part from outside that chain. The latter is of course true only within the set of substitutable parts we set out with. We hypothesize that:

\[ \text{H4: Parts that have higher distribution flexibility have lower counterfeit risk.} \]

6.2 Managing lead time

Lead time management can be done by having additional inventory and/or capacity as well as by utilizing faster delivery modes in transportation. Although we do not observe inventory and capacity buffers directly in our data (we only observe the authorized distributor inventories), we would expect that when a disruption
in supply occurs, parts with higher buffer would experience a relatively lower increase in lead time. Thus, we observe the consequence of building buffers in the supply chain through its impact on lead time.

In Section 5, we show that parts that have a high lead time (top quartile) and higher positive trend in lead time (top two quartiles) have a higher probability of being counterfeited. Thus, manufacturers can mitigate their counterfeit risk by proactively managing the lead times of these parts in particular. They can institute alert systems and work with distributors for keeping lead times in check.

For such risky parts, manufacturers and distributors could also guide customers to substitute parts that are readily available. Since demand is shifted within the authorized distribution network, these substitute parts come with similar guarantees on authenticity of the part and warranty support. As a result, the distribution network can provide an additional buffer against counterfeit risk when there are substitute parts available within a short lead time. We capture this lead time buffer through the difference between the average lead time for the part and the minimum lead time among all substitutable parts in the distribution network. Hence, we hypothesize that:

\[ H5: \text{Parts that have higher lead time buffer in the distribution network have lower counterfeit risk.} \]

6.3 Sharing information

For the electronics industry, with endemic uncertainty on both demand and supply sides, Lee (2002) highlights information sharing between supply chain partners as an effective way to coordinate along the supply chain. This includes suppliers sharing information on production/delivery schedules, order tracking, and capacity information. Further, when there is a long-term relationship between supply chain partners, the information shared tends to be credible (Ren et al. 2010) and valuable (Lee et al. 2000), while information delays can lead to lower supply chain performance (Chen 1999). Collaboration between supply chain partners based on shared demand information can lead to better forecasts of demand (Aviv 2001), sharing information on production delays can help customers adapt their production schedules and prevent potential shortage gaming behavior (Lee et al. 1997).

In our context, manufacturers use change notifications (first introduced on p. 7) to communicate information on part changes and the corresponding impact of these changes on the supply and distribution of these parts. Such communication would include reason for the change, details on the extent and duration of the impact, and alternate solutions. Manufacturers also proactively communicate upcoming changes to the supply base and manufacturing process to their customers. Thus, change notifications help customers manage their operations better in the face of potential shortages that in turn would reduce the likelihood of purchase of parts outside the authorized distribution network. Hence, we hypothesize that:
Higher levels of information sharing on upcoming changes to the part with downstream supply chain members lowers the counterfeit risk for a part.

6.4 Empirical analysis of operational strategies to mitigate counterfeit risk

To test H4-H6, we define the following additional variables for each of the above risk mitigation strategies.

**Distribution Flexibility ($DF_i$)** – We calculate the distribution flexibility measure for each part as follows: First, we create a link between parts and the authorized distributors where each of these parts are held. Next, we adapt the process flexibility measure from Graves and Tomlin (2003) to calculate the distribution flexibility for each part (basic definitions are in Section 6.1). As pointed out earlier, the part distribution flexibility $g_i$ is a relative measure, hence it is appropriate to compare distribution flexibility across parts within the same network. However, in our setting we have multiple networks. To enable comparison across networks, we make two modifications. First, we normalize the part distribution flexibility measure ($g_i$) as $DF_i = \left(g_i + 1\right) \times I = \left(\sum_{j \in P(i)} c_j\right) / \left(\sum c_j\right)$. The normalized measure is simply the fraction of total (substitutable) inventory that the part has access to. Second, we control for network fixed effects $N_n$ in our empirical specification. This serves to capture the impact of the distribution network flexibility measure $g$ without having to enumerate over all possible subsets.

**Lead time buffer in the network** ($L_M_i$) – This is the differential between the part lead time ($L_i$) and the minimum lead time amongst all substitutable parts in the distribution network ($n$).

**Information Sharing** ($IS_i$) – This is the ratio of the number of change notifications issued for part $i$ to the number of changes made to part $i$.

We add the above variables on risk mitigation to our outcome equation as shown below:

\[
CR_i = \alpha_0 + \alpha_1 S_i + \alpha_2 L Q_i + \alpha_3 L TQ_i + \alpha_4 P_i + \alpha_5 PD_i + \alpha_6 U_i + \alpha_7 EC_i + \alpha_8 IC_i + \rho_1 PC_{cf} + \rho_2 Y_i + \rho_3 PP_i + \rho_4 W_{fcn} + \delta_1 DF_i + \delta_2 L M_i + \delta_3 IS_i + \varepsilon_i \tag{5}
\]

The results of the estimation are shown in Table 2, column C2. We find that the coefficients for distribution flexibility ($DF_i; \delta_1$), lead time buffer ($L_M_i; \delta_2$), and information sharing ($IS_i; \delta_3$) to be negative and significant ($p<0.01$), indicating that higher levels of distribution flexibility, larger lead time buffer in the network, and more information sharing are all effective in mitigating counterfeit risk. Thus we find strong support for H4-H6.

6.5 Are these operational strategies substitutes or complements?

In this section, we investigate if these operational strategies substitute or complement each other. To do this, we introduce two-way interactions among distribution flexibility, lead time (trend in lead time and lead time buffer in the network), and information sharing to our outcome equations as shown in equation (6). We “mean-center” the variables involved in interaction terms so that the individual coefficients for the direct effects of these variables reflect the effect when the other two variables are set to their average values.
\[ CR_i = \alpha_0 + \alpha_1 S_i + \alpha_2 L.TQ_i + \alpha_3 P_i + \alpha_4 P_i D_i + \alpha_5 U_i + \alpha_6 E_i + \alpha_7 C_i + \alpha_8 I_i + \rho_1 P_{cf} \]
\[ + \rho_2 Y_i + \rho_3 P_{PP} + \rho_4 W_{fcn} + \delta_1 D_{Fi} + \delta_2 L.M_i + \delta_3 I.S_i + \gamma_1 D_{Fi} \times L.TQ_i + \gamma_2 D_{Fi} \times L.M_i + \gamma_3 D_{Fi} \times I.S_i + \gamma_4 I.S_i \times L.TQ_i + \varepsilon_i \]  

The results of our estimation are available in Table 2, column C3. We find that the interaction term between distribution flexibility and top quartile for trend in lead time to be negative and significant \((DF_i \times L.TQ_i; \gamma_1)\) \((p<0.001)\). This indicates that it is easier to source alternate parts to fulfill a shortfall in supply when there is higher distribution flexibility. Next, we find that the interaction term between distribution flexibility and information sharing \((DF_i \times I.S_i; \gamma_3)\) is negative and significant \((p<0.001)\), indicating that an increase in distribution flexibility helps improve the effectiveness of information sharing. Further, the interaction term between distribution flexibility and lead time buffer for parts in the network is negative and significant \((DF_i \times L.M_i; \gamma_2)\) \((p<0.01)\). This indicates that distribution flexibility complements the impact of lead time buffer available and in the network. Finally, we also find the interaction term between the top quartile for lead time and information sharing \((I.S_i \times L.TQ_i; \gamma_4)\) to be negative and significant \((p<0.01)\), indicating the information sharing can help moderate the impact of lead time increase on counterfeit risk for parts with relatively high lead times.

### 6.6 Quantitative assessment

We conduct a quantitative assessment of our models through the marginal effects routine in STATA using the coefficients from Table 2, column C3 (the full model). First, we look at the direct impact of operational strategies in reducing counterfeit risk. We find that a one-standard-deviation increase in distribution flexibility and information sharing (ceteris paribus, each on its own) reduces counterfeit risk by 11.14% and 22.92%, respectively. The results on the lead time buffer needs to be interpreted with caution. We find that there are two different ways lead time can impact counterfeit risk. First, parts that have high lead time and higher positive trend in lead time have a higher probability of counterfeit risk (from Section 5.3). For these parts, we estimate that a 20% reduction in average lead time and trend in lead time (ceteris paribus, each on its own) would directly lower counterfeit risk by 4.40% and 3.73%, respectively. Second, we observe that for these parts, increasing the lead time buffer by 20% leads to a 2.32% reduction in counterfeit risk. Taken together, this indicates that (1) direct lead time management can effectively reduce counterfeit risk, and (2) for high-lead-time parts, counterfeit risk can be reduced by being part of a distribution network with high lead time buffer.

Next, we look at the combined impact of these operational strategies on counterfeit risk. In quantitative terms, when there is a higher positive trend in lead time, distribution flexibility lowers counterfeit risk by 15.93% (i.e., an additional 4.79% compared to the average). We also find that a one-standard-deviation increase in distribution flexibility helps improve the effectiveness of information sharing by 9.81%, i.e., it complements the effect of information sharing. As information sharing allows customers to prepare for
upcoming changes, with higher distribution flexibility, they can proactively source alternate parts from the distribution network. Finally, for parts that have a higher positive trend in lead time, increased information sharing can reduce counterfeit risk for parts by an additional 3.71%. This indicates that information sharing on upcoming changes that could lead to an increase in lead time for the part can be valuable in reducing counterfeit risk, as it gives customers time to plan for these changes ahead of time.

7 Robustness tests

7.1 Alternate network specifications

In Sections 5 and 6, we created a network of substitutable parts to calculate the distribution flexibility for each part in the network. This assumes perfect (or 100%) substitution across parts within the network. In this section, we test the robustness of our assumption. FPGA parts differ from each other on three major dimensions – parametric data (e.g., operating voltage and frequency, logic blocks, etc.), package options (e.g., frame, pin count, dimensions, etc.), and environmental compliance (e.g., compliance with RoHS, lead free, etc.). These could potentially lead to imperfect substitution among the parts and influence the distribution flexibility measure. We conducted the following tests to see if the above assumptions may have a significant impact on our results.

We created alternate networks of substitutable parts based on (1) same parametric data, (2) similar package options, and (3) environmental compliance. To account for environmental compliance, we split each network into parts that were environmentally compliant and parts that were not compliant. We calculate the distribution flexibility measure (as in Section 6.1) for parts within each of these re-defined networks and conduct the same analysis as in Section 6.4. We find that our main results on the impact of distribution flexibility on counterfeit risk continue to hold with each of these alternate network specifications.

7.2 Alternate methods to calculate distribution flexibility

First, we look at a measure that normalizes the inventory held at each distributor to 1. This would be helpful in situations where inventory information may not be available or accurate. In such a scenario, the distribution flexibility captures the number of different distributors that are available in the connected network. Second, we use the number of links in the network as our distribution flexibility measure. We find qualitatively similar results with both methods.

7.3 Alternate cutoff points for counterfeit reports

In Section 5, we considered a 6 month period after the cut-off date to determine if there were any counterfeit reports for the part. We tested the robustness of our results by looking at counterfeit reports released 3 months, 9 months and 1 year after the cut-off date. We find qualitatively similar results with different time-windows.
8 Managerial and policy implications

In this section, we discuss practical implications of our analysis and results. We start with implications of our study for individual supply chain members – manufacturers, distributors, and customers. Next, we expand on how our results can inform policy makers on the effectiveness of standards and regulations towards combating the risk of counterfeit electronics.

8.1 Implications for managers

We start with the implications of our study for manufacturers, distributors, and customers in the FPGA supply chain. First and foremost, our results highlight the role of distribution flexibility – ability to shift order fulfillment from one product or distributor to another – in mitigating counterfeit risk (H4). We find that a one-standard-deviation increase in distribution flexibility reduces counterfeit risk by 11.14%. There are at least two different ways in which distribution flexibility can be increased: (1) increasing inventory for the part at the distributor, and (2) increasing the number of distributors for the part. When we increase inventory for the focal part, its part-flexibility as well as part-flexibility for other parts that are held alongside the focal part increases (a spillover effect), while part-flexibility for other parts in the network decrease. When we increase the number of distributors for a focal part (while maintaining the same inventory level), it increases part-flexibility for the focal part as well as for other parts held at the new distributor. Thus, from a manufacturer’s perspective, it would be more beneficial to increase the number of distributors and/or increase inventory for a part (or set of parts) that have the most overlap with other parts from the same manufacturer in the same network in order to reduce the counterfeit risk for their parts. If the manufacturer has only one part, then it would be most beneficial to add a distributor that carries the most number of parts. In our sample, the average number of distributors per part is 4.21. A one-standard deviation increase in distribution flexibility can be achieved by adding an additional distributor (without increasing the overall inventory level) for parts that are held at 2 or fewer distributors. However, benefits of decreased counterfeit risk by holding higher inventory or increasing the number of distributors needs to be balanced against an increase in holding and obsolescence costs due to carrying higher inventory and an increase in transportation and transaction costs arising from more distributors in the network.

We offer empirical evidence for two other mitigation strategies: Managing part lead times, and sharing information with downstream supply chain members. It is clear from our results (and intuitive) that parts with really long lead times are the ones managers must pay attention to (H1). We also argue (in H5) that parts enjoying the safety net of a substitute part within a short lead time are less vulnerable to counterfeiting. This raises a tension between acting on competitive instincts and minimizing counterfeit risk: Some demand going to substitute parts, hence losing business to competitors, may have a silver lining in that keeping the customer within the authorized network may prevent counterfeit parts entering the supply chain. Our work
shines a light on this tension and suggests that manufacturers and their authorized distributors must find collaborative ways to resolve it in practice if they want to fight counterfeits.

Another takeaway from our results is that information sharing helps a lot. Generically speaking, any perturbation to the usual functioning of the supply chain may increase its exposure to counterfeit risk. We establish external changes as one such perturbation (H3). Manufacturers are often wary of releasing information on upcoming changes to the part, especially if it is a supply chain related problem. Based on H6, we then show that it is not the part changes themselves, but the lack of information that downstream supply chain members have about them that really increases the counterfeit risk for manufacturers. Therefore, manufacturers need not avoid change, but they must communicate any part change to their distributors and customers as soon as they can. Otherwise – our results show – the supply chain will be strained to keep supply of parts within the authorized distribution network, hence raising the specter of counterfeiting.

An unintended consequence of purchase and subsequent failure due to a counterfeit part is that it often gets returned back to the manufacturer (i.e., the customer assumes it is a genuine part and sends it back to the manufacturer). The manufacturer then has to spend time and resources to test the cause of failure before determining it to be a counterfeit part (e.g., Cisco claimed USD 27 million as compensation in false warranty claims for fake parts) (Duffy 2007; Hochmuth 2007; Tung 2011). In addition to incurring the cost of testing the part, the manufacturer also suffers a loss of reputation in the market. Thus, our results show that these operational strategies could potentially help the manufacturer save on costs of dealing with counterfeit parts.

8.2 Implications for policy makers

Next, we discuss implications of our study with respect to government policy and regulations that could impact counterfeit risk. In the electronics industry context, environmental regulations like RoHS (restriction of hazardous substance), RoHS2, REACH (registration, evaluation, authorization, and restriction of chemicals) etc. have brought about a significant change in the kind of materials and processes used to manufacture electronic components. This causes a two-fold impact on the electronic component supply chain. First, change in material or process to comply with regulations requires the manufacturers to find suppliers that could produce the compliant parts. This takes time and resources and can create temporary shortages. This provides an opportunity for counterfeit (non-compliant) parts to enter the supply chain. We find support for this in our results where external changes have a significant impact on counterfeit risk. Second, non-compliant parts at the customer (OEMs) have to be removed from the supply chain. This is done through recycling or selling them to the lowest cost bidder. Often these are functional parts and if they are not recycled or destroyed completely, they land in the hands of counterfeiters. This happens several tiers down the supply chain and many customers rarely keep record of how parts are recycled beyond the
immediate tier (Sheffi 2005, Chen et al. 2017). With small modifications to label and appearance, these non-compliant parts are sold by counterfeiters as “compliant parts” thus creating the problem of counterfeits. Although there is no known database that lists all the available counterfeit parts in the market, in close to 60% of the reports we find that an older version of the genuine part was used to produce the counterfeit part. Thus, environmental regulations that involve large-scale disposal of functioning parts and those that affect many supply chain members to ensure compliance can have the unintended consequence of increasing counterfeit parts entering the supply chain. Policy makers must take steps to prevent such unintended consequences.

Finally, we discuss how development of standards can help mitigate the risk of counterfeit parts entering the supply chain. Unauthorized sources in the electronics industry span a wide spectrum of distributors and brokers. Many big-name independent distributors have sought to differentiate themselves by creating standards that outline the necessary steps to ensure authenticity of parts. For example, TTI, Digi-key and a few other independent distributors have been instrumental in crafting a certification standard for independent distributors to ensure authenticity of the part. This involves auditing sub-tier suppliers, conducting multiple functional tests to ensure authenticity of the parts, and maintaining a document trail as the part moves through the supply chain. All of these activities are expected to increase procurement and overhead cost for the distributor. However, these distributors may find it hard to pass these costs onto the customer as our results indicate that relative price difference is significantly associated with purchase of counterfeit parts (H2). Instead, the distributors could charge similar prices as the authorized distributors if they can institute deferred payments (full payment made after the product is verified as genuine) as a way to build confidence in their products. Thus, we provide a practical application for the deferred payment mechanism proposed by Babich and Tang (2012) as a way to combat counterfeits. We observe some initial efforts in this regard where distributors have been involved in developing certification protocols and have offered to hold customer payments in escrow till the parts pass the inspection at the customer’s site (e.g., ERAI’s escrow services).

9 Conclusions, limitations, and future work

In this paper, we analyze supply chain risk factors that drive counterfeit risk and quantify the effectiveness of distribution flexibility, lead time management, and information sharing towards mitigating this risk. Our main findings are: (1) high-value parts have an increased risk of being counterfeited; (2) increase in the price difference between authorized distributors and unauthorized sources, higher number of external changes that entail significant changes to the supply chain, and significant increase in lead time lead to an increase in counterfeit risk for the part; and (3) increased distribution flexibility, that allows distributors to guide customers to substitute parts within the network, reduces counterfeit risk by 11.14% on average. Further, when there is a significant increase in lead time, distribution flexibility lowers counterfeit risk by 15.93% (i.e., an additional 4.79% compared to the average) and increase in distribution flexibility increases effectiveness of information sharing by 9.81%. Finally, increased information sharing for parts that
experience a significant increase in their lead time reduces counterfeit risk by 13.77%. These findings help manufacturers and distributors understand operational strategies they can use to proactively reduce counterfeit risk. Our findings also have policy implications for the industry in terms of regulations, development of standards, and incentivizing supply chain members to source responsibly that would mitigate the threat of counterfeit parts in the electronics component supply chain.

Our study uses a unique dataset on part information, authorized distribution network, unauthorized sources, and counterfeit reports. However, we only have a single snapshot of this information in time. With a panel data it would be possible to see how the counterfeit risk changes over time. Further, we do not have access to capacity decisions made by manufacturers and the ordering and inventory management policies at each of the distributors. We only observe the consequence of these decisions through information on ending inventory (or shortages) and lead time. Information on the policies adopted by manufacturers and distributors to manage capacity and inventory could help understand if there were systematic factors in these decisions that lead to shortages. Finally, our work does not distinguish between substitutes available from the same manufacturer and from competitors. It is possible that there may be a higher transaction cost involved in sourcing parts from a different manufacturer even via the same distributor. Future work could look at these issues as more information becomes available.

References:


Figures and Tables:

Figure 1: Electronic component supply chain

![Supply chain diagram]

Figure 2: Timeline of events

![Timeline diagram]

Figure 3: Distribution networks with more links have higher distribution flexibility.

![Distribution network diagrams]
Table 1: Summary statistics

<table>
<thead>
<tr>
<th>Variable</th>
<th>Average</th>
<th>Standard deviation</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeit reports (#)</td>
<td>0.36</td>
<td>0.75</td>
<td>0.00</td>
<td>8.00</td>
</tr>
<tr>
<td>Change notifications (#)</td>
<td>3.00</td>
<td>1.11</td>
<td>1.00</td>
<td>6.00</td>
</tr>
<tr>
<td>Distribution flexibility</td>
<td>0.39</td>
<td>0.32</td>
<td>0.00</td>
<td>1.00</td>
</tr>
<tr>
<td>External changes (#)</td>
<td>6.23</td>
<td>1.78</td>
<td>2.00</td>
<td>11.00</td>
</tr>
<tr>
<td>Information sharing</td>
<td>0.48</td>
<td>0.11</td>
<td>0.15</td>
<td>0.57</td>
</tr>
<tr>
<td>Internal changes (#)</td>
<td>8.19</td>
<td>3.45</td>
<td>3.00</td>
<td>23.00</td>
</tr>
<tr>
<td>Inventory (units)</td>
<td>257.31</td>
<td>654.14</td>
<td>0.00</td>
<td>15000</td>
</tr>
<tr>
<td>Lead time (weeks)</td>
<td>11.00</td>
<td>17.50</td>
<td>1.00</td>
<td>52.00</td>
</tr>
<tr>
<td>Prior counterfeit reports for part-category (#)</td>
<td>51.65</td>
<td>65.19</td>
<td>3.00</td>
<td>127.00</td>
</tr>
<tr>
<td>Price ($)</td>
<td>25.75</td>
<td>10.17</td>
<td>5.21</td>
<td>76.44</td>
</tr>
<tr>
<td>Price difference ($)</td>
<td>10.00</td>
<td>16.60</td>
<td>0.00</td>
<td>25.70</td>
</tr>
<tr>
<td>Shortage</td>
<td>0.31</td>
<td>0.55</td>
<td>0.16</td>
<td>1.00</td>
</tr>
<tr>
<td>Substitutes (# within a network)</td>
<td>21.04</td>
<td>35.22</td>
<td>12.00</td>
<td>158.00</td>
</tr>
<tr>
<td>Trend in lead time (weeks)</td>
<td>3.11</td>
<td>5.21</td>
<td>0.00</td>
<td>21.65</td>
</tr>
<tr>
<td>Unauthorized sources (#)</td>
<td>7.89</td>
<td>5.11</td>
<td>0.00</td>
<td>27.00</td>
</tr>
<tr>
<td>Years since introduction (# of years)</td>
<td>4.30</td>
<td>2.21</td>
<td>0.20</td>
<td>10.50</td>
</tr>
</tbody>
</table>
Table 2: Estimation results for supply chain drivers of counterfeit risk and impact of mitigation strategies.

<table>
<thead>
<tr>
<th>Variable</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection Chi-Square</td>
<td>101.3487***</td>
<td>102.1198***</td>
<td>105.8191***</td>
</tr>
<tr>
<td>N</td>
<td>6905</td>
<td>6905</td>
<td>6905</td>
</tr>
<tr>
<td>Years since introduction (0.03143)</td>
<td>0.07291***</td>
<td>0.07254***</td>
<td>0.07181***</td>
</tr>
<tr>
<td>Price ($)</td>
<td>0.05718**</td>
<td>0.05709**</td>
<td>0.05765**</td>
</tr>
<tr>
<td>Prior reports for part-category (#)</td>
<td>0.03285*</td>
<td>0.03277*</td>
<td>0.03271*</td>
</tr>
<tr>
<td>Average leadtime (weeks)</td>
<td>0.00251 (0.06825)</td>
<td>0.00250 (0.06798)</td>
<td>0.00248 (0.06113)</td>
</tr>
<tr>
<td>Average part popularity</td>
<td>0.03191 (0.0521)</td>
<td>0.03367 (0.03381)</td>
<td>0.03654 (0.04082)</td>
</tr>
<tr>
<td>Constant</td>
<td>1.18718***</td>
<td>1.18711***</td>
<td>1.18707***</td>
</tr>
<tr>
<td>(0.01923)</td>
<td>0.01922)</td>
<td>(0.01909)</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>6905</td>
<td>6905</td>
<td>6905</td>
</tr>
<tr>
<td>Price of part</td>
<td>(0.00891)</td>
<td>(0.00882)</td>
<td>(0.00661)</td>
</tr>
<tr>
<td>DF * Trend in lead time (3rd quartile)</td>
<td>-0.42571***</td>
<td>-0.34812***</td>
<td></td>
</tr>
<tr>
<td>DF * Trend in lead time (4th quartile)</td>
<td>-0.00524*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DF * Lead time buffer from network</td>
<td>-0.13623*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DF * IS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS * Trend in lead time (3rd quartile)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS * Trend in lead time (4th quartile)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Popular part (Y/N)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Years since introduction (0.19811)</td>
<td>-0.27789 (0.19811)</td>
<td>-0.15801 (0.19697)</td>
<td>-0.15779 (0.19973)</td>
</tr>
<tr>
<td>Constant</td>
<td>0.34921***</td>
<td>0.36151***</td>
<td>0.36151***</td>
</tr>
<tr>
<td>(0.02189)</td>
<td>(0.02277)</td>
<td>(0.02277)</td>
<td></td>
</tr>
<tr>
<td>Part category, network, firm fixed effects</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Log-likelihood</td>
<td>-3181.9521</td>
<td>-3029.7612</td>
<td>-3029.7612</td>
</tr>
<tr>
<td>N</td>
<td>6905</td>
<td>6905</td>
<td>6905</td>
</tr>
</tbody>
</table>

*p<0.05, **p<0.01, ***p<0.001, standard errors are in parentheses.